



## 【特許請求の範囲】

## 【請求項 1】

コンテンツをライセンス供与する方法であって、  
ライセンス要求を受け取るステップであって、前記ライセンス要求はライセンスの交付を受けるエンティティについての識別証明書を含み、前記識別証明書は前記識別証明書を交付した交付者を示すステップと、  
前記識別証明書の前記交付者を信用すると決定するステップと、  
前記コンテンツを前記エンティティにライセンス供与するための条件が存在すると決定するステップと、  
前記コンテンツを前記エンティティが使用するためのライセンスを生み出すステップと、  
前記ライセンスを前記エンティティに送るステップと  
を含むことを特徴とする方法。

10

## 【請求項 2】

前記識別証明書は、(a) 前記交付者に関連する公開鍵証明書と (b) 前記交付者のデジタル署名とを含み、  
前記公開鍵証明書を使用して前記デジタル署名を検証するステップをさらに含むことを特徴とする請求項 1 に記載の方法。

## 【請求項 3】

前記ライセンス要求は、ライセンスを交付できるライセンス供与条件を示す権利データを含み、前記コンテンツをライセンス供与するための条件が存在すると決定する前記ステップは前記権利データに基づくことを特徴とする請求項 1 に記載の方法。

20

## 【請求項 4】

前記識別証明書は、公開鍵を含み、前記公開鍵に対応する秘密鍵を含むかまたは前記秘密鍵に関連付けられ、ライセンスを生み出す前記ステップは、  
前記公開鍵を使用して前記コンテンツのための復号鍵を暗号化して、暗号化済み復号鍵を生成するステップと、  
前記暗号化済み復号鍵を前記ライセンスに含めるステップと  
を含むことを特徴とする請求項 1 に記載の方法。

## 【請求項 5】

前記識別証明書は、公開鍵を含み、前記公開鍵に対応する秘密鍵を含むかまたは前記秘密鍵に関連付けられ、ライセンスを生み出す前記ステップは、  
対称鍵を使用して前記コンテンツのための復号鍵を暗号化して、暗号化済み復号鍵を生成するステップと、  
前記対称鍵を前記公開鍵で暗号化して、暗号化済み対称鍵を生成するステップと、  
前記暗号化済み対称鍵と前記暗号化済み復号鍵の両方を前記ライセンスに含めるステップと  
を含むことを特徴とする請求項 1 に記載の方法。

30

## 【請求項 6】

前記方法は信用される交付者のリストを維持するサーバによって実施され、前記識別証明書の前記交付者を信用すると決定する前記ステップは、前記交付者が前記リスト上にあるかどうかを決定するステップを含むことを特徴とする請求項 1 に記載の方法。

40

## 【請求項 7】

前記信用される交付者はそれぞれ対応する公開鍵証明書を有し、前記リストは前記信用される交付者についての公開鍵証明書のリストを含み、  
前記交付者の公開鍵証明書が前記リスト上にあるかどうかを決定するステップを含むことを特徴とする請求項 6 に記載の方法。

## 【請求項 8】

前記交付者は e メールアドレスおよびパスワードに基づいて公衆に識別証明書を交付するサーバであると決定するステップであって、前記証明書は e メールアドレスを示すステップと、

50

前記メールアドレスも、前記メールアドレス中で識別されるドメイン名も、除外リスト上にないと決定するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 9】

前記交付者に対して適用可能な除外リストが存在すると決定するステップと、

前記除外リストの条件に基づいて前記識別証明書が除外されないと決定するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 10】

前記除外リストは 1 つまたは複数のメールアドレスを含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上のメールアドレスを指定する識別証明書に対しては、ライセンスは交付されない場合があり、

前記識別証明書が前記除外リスト上のメールアドレスを指定していないと決定するステップを含む

ことを特徴とする請求項 9 に記載の方法。

【請求項 11】

前記除外リストは 1 つまたは複数のドメイン名を含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上のドメイン名を指定する識別証明書に対しては、ライセンスは交付されない場合があり、

前記識別証明書が前記除外リスト上のドメイン名を指定していないと決定するステップを含む

ことを特徴とする請求項 9 に記載の方法。

【請求項 12】

前記除外リストは 1 つまたは複数の識別子を含み、したがって、前記交付者によって交付された識別証明書であって前記除外リスト上の識別子を含む識別証明書に対しては、ライセンスは交付されない場合があり、

前記識別証明書が前記除外リスト上の識別子を含まないと決定するステップを含むことを特徴とする請求項 9 に記載の方法。

【請求項 13】

請求項 1 に記載の方法を実施するためのコンピュータ実行可能命令を有することを特徴とするコンピュータ可読媒体。

【請求項 14】

コンテンツをライセンス供与する方法であって、

権利ラベルを含むライセンス要求を受け取るステップを含み、前記権利ラベルは、

前記権利ラベルを交付したエンティティを示すデータと、前記エンティティに関連する秘密鍵を使用して復号可能な形の、前記コンテンツのための暗号化済み復号鍵と

を含み、方法はさらに、

前記秘密鍵が利用可能であると決定するステップと

前記秘密鍵を使用して前記暗号化済み復号鍵を復号し、それにより前記コンテンツのための復号鍵を生成するステップと、

暗号化された形の前記復号鍵を含むライセンスを生み出すステップと、

前記ライセンスをライセンス取得側に送るステップと

を含むことを特徴とする方法。

【請求項 15】

前記権利ラベルを交付する前記エンティティは関連する公開鍵証明書を有し、前記権利ラベルを交付したエンティティを示す前記データは前記公開鍵証明書を含むことを特徴とする請求項 14 に記載の方法。

【請求項 16】

前記暗号化済み復号鍵は、前記権利ラベルを交付した前記エンティティに関連する公開鍵で暗号化されることを特徴とする請求項 14 に記載の方法。

【請求項 17】

10

20

30

40

50

前記暗号化済み復号鍵は対称鍵で暗号化され、前記権利ラベルはさらに、  
 前記権利ラベルを交付した前記エンティティに関連する公開鍵で暗号化された前記対称鍵  
 を含み、  
 前記秘密鍵を使用して前記暗号化済み復号鍵を復号する前記ステップは、  
 前記秘密鍵を使用して前記対称鍵を復号するステップと、  
 前記対称鍵を使用して前記復号鍵を復号するステップと  
 を含むことを特徴とする請求項 14 に記載の方法。

【請求項 18】

前記権利ラベルを交付した前記エンティティが信用できると決定するステップをさらに含  
 むことを特徴とする請求項 14 に記載の方法。

【請求項 19】

前記ライセンス取得側は公開／秘密鍵の対に関連し、ライセンスを生み出す前記ステップ  
 は、

前記公開／秘密鍵の対の公開部分で前記復号鍵を暗号化するステップを含む  
 ことを特徴とする請求項 14 に記載の方法。

【請求項 20】

前記権利ラベルに署名した前記エンティティから前記秘密鍵を受け取るステップをさらに  
 含むことを特徴とする請求項 14 に記載の方法。

【請求項 21】

前記方法を実施する前記エンティティは公開／秘密鍵の対に関連し、前記秘密鍵は、前記  
 公開／秘密鍵の対の公開部分で暗号化された形で、前記権利ラベルに署名したエンティテ  
 ィから受け取られることを特徴とする請求項 20 に記載の方法。

【請求項 22】

請求項 14 に記載の方法を実施するためのコンピュータ実行可能命令を有することを特徴  
 とするコンピュータ可読媒体。

【請求項 23】

コンテンツをライセンス供与するためのシステムであって、  
 信用されるエンティティのリストと、  
 ライセンス交付モジュールと

を備え、前記ライセンス交付モジュールは、ライセンスの交付を受ける識別についての識  
 別証明書を含むライセンス要求を受け取り、前記識別証明書が前記信用されるエンティテ  
 ィのうちの 1 つによって交付されたものかどうかを決定し、前記コンテンツをライセンス  
 供与するための条件が満たされるかどうかを決定し、前記識別証明書が前記信用されるエ  
 ンティティのうちの 1 つによって交付されたものである場合であって前記コンテンツをラ  
 イセンス供与するための条件が満たされる場合に、ライセンスを交付することを特徴とす  
 るシステム。

【請求項 24】

前記信用されるエンティティはそれぞれ、関連する公開／秘密鍵の対と、前記公開／秘密  
 鍵の対の公開部分についての公開鍵証明書とを有し、前記信用されるエンティティのリス  
 トは、前記信用されるエンティティそれぞれについての公開鍵証明書を含むことを特徴と  
 する請求項 23 に記載のシステム。

【請求項 25】

前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの 1 つ  
 のデジタル署名を含み、前記ライセンス交付モジュールは、前記リスト中の前記公開鍵  
 証明書のうちの 1 つを使用して前記デジタル署名を検証することを特徴とする請求項 2  
 4 に記載のシステム。

【請求項 26】

前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの 1 つ  
 についての公開鍵証明書を含み、前記ライセンス交付モジュールは、前記識別証明書中の  
 前記公開鍵証明書を前記リスト上の前記公開鍵証明書と比較することにより、前記識別証

10

20

30

40

50

明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項 24 に記載のシステム。

【請求項 27】

前記信用されるエンティティはそれぞれ関連する識別子を有し、前記信用されるエンティティのリストは、前記信用されるエンティティそれぞれについての識別子を含むことを特徴とする請求項 23 に記載のシステム。

【請求項 28】

前記識別証明書は、前記識別証明書を交付した前記信用されるエンティティのうちの 1 つについての識別子を含み、前記ライセンス交付モジュールは、前記識別証明書中の前記識別子を前記リスト上の前記識別子と比較することにより、前記識別証明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項 27 に記載のシステム。

10

【請求項 29】

前記信用されるエンティティはそれぞれ、関連する公開／秘密鍵の対と、前記公開／秘密鍵の対の公開部分についての公開鍵証明書とを有し、前記信用されるエンティティのリストは、前記信用されるエンティティそれぞれについての前記公開鍵証明書を含み、前記識別証明書はさらに、前記識別証明書を交付した前記信用されるエンティティのうちの 1 つについての公開鍵証明書を含み、前記ライセンス交付モジュールはさらに、前記識別証明書中の前記公開鍵証明書を前記リスト上の前記公開鍵証明書と比較することにより、前記識別証明書が信用されるエンティティによって交付されたものかどうかを決定することを特徴とする請求項 28 に記載のシステム。

20

【請求項 30】

コンテンツをライセンス供与するためのシステムであって、前記コンテンツには、前記コンテンツのための暗号化済み復号鍵を含む権利ラベルが関連し、前記暗号化済み復号鍵は復号可能であり、

それぞれが特定の発行エンティティに関連する秘密鍵のセットと、

ライセンス交付モジュールと

を備え、前記ライセンス交付モジュールは、どの発行エンティティが前記権利ラベルを交付したかを決定し、前記権利ラベルを交付した前記発行エンティティの秘密鍵を前記秘密鍵のセットが含むかどうかを決定し、前記発行エンティティの秘密鍵を使用して前記暗号化済み復号鍵を復号して、前記コンテンツのための復号鍵を生成し、前記コンテンツのための前記復号鍵を含むライセンスを生み出すことを特徴とするシステム。

30

【請求項 31】

前記ライセンスは、暗号化された形で前記コンテンツのための前記復号鍵を含むことを特徴とする請求項 30 に記載のシステム。

【請求項 32】

前記権利ラベルは、前記権利ラベルを交付した発行エンティティの証明書を含み、前記ライセンス交付モジュールは、前記証明書に基づいて、前記セット中のどの秘密鍵が、前記権利ラベルを交付した前記発行エンティティに対応するかを識別することを特徴とする請求項 30 に記載のシステム。

40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル権利管理システムに関する。より詳細には、本発明は、権利を管理するコンテンツに対するライセンスを誰が受けることができるか、および誰がこのようなライセンスを交付することができるかを、信用モデルを使用して定義することに関する。

【0002】

【従来の技術】

デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディア、ソフトウェアなどのデジタルコンテンツを 1 人または複数の

50

ユーザに配布する場合、このようなデジタルコンテンツに関してはデジタル権利管理（「DRM」）および施行が非常に望ましい。デジタルコンテンツは、例えばテキスト文書などのように静的なこともあり、ライブイベントのストリーミングオーディオ／ビデオなどのようにストリーミングされることもある。権利管理システムの典型的な使用法では、ユーザがネットワーク（例えばインターネット）を介して、または物理媒体上で（例えばディスク上で）、デジタルコンテンツを受け取る。さらに、ユーザがコンテンツを「消費」すること（例えばオーディオまたはビデオコンテンツの再生、テキストコンテンツの閲覧、ソフトウェアの実行など）が許可される場合、ユーザはこのようなコンテンツに対するライセンスも受ける。権利管理システムは、ライセンスの条件によってこのような消費が許可されるときだけユーザがコンテンツを消費できるという要件を施行する。

10

#### 【0003】

権利管理システムは通常、少なくとも2つのコンテキストで暗号に依存する。第1に、保護する必要があるコンテンツが暗号化される。第2に、暗号化されたコンテンツを有意に使用するために復号鍵が必要な場合、鍵は信用されるエンティティだけに配布しなければならず、この信用は暗号証明書および署名を使用して確立される。最も単純な権利管理システムでは、暗号化されたコンテンツの所有者が、このコンテンツの消費者の信用性を直接に検証し、所有者が消費者の信頼性を確信すれば、復号鍵を含むライセンスをこの消費者に配布する。しかし、このようなシステムは、大きな商業的意義を有するまでに十分豊富な機能は提供しない。ほとんどのコンテンツは、商業における他のどんなものもそうであるように、複雑な関係のチェーン（連鎖）またウェブを介して配布される。例えば、コンテンツ所有者は、コンテンツに対するライセンス（したがって鍵）を交付する作業を実際にはディストリビュータに委任する場合がある。この場合、コンテンツ所有者とライセンスディストリビュータとを分離することにより、コンテンツをどのように配布するかに関しより大きなフレキシビリティがもたらされる（例えばコンテンツ所有者は、コンテンツを配布しライセンス供与サーバを運営することによって時間または金銭を費やす必要がない）。一方、この分離はまた、コンテンツ所有者（コンテンツの所有権を有する）がライセンスディストリビュータ（所有者の所有権に影響力を有する）を信用することを必要とする。

20

#### 【0004】

配布／権利管理プロセスの他の面も分離することができ。例えば、ライセンス供与側は、特定のハードウェアプラットフォーム上でコンテンツを消費することをユーザに許可するライセンスを交付する場合、（a）ユーザの識別（ライセンス供与が特定のユーザに限定される場合）と、（b）コンテンツが消費されることになるプラットフォームのセキュリティとについて暗黙的に決定を行っている。ライセンス供与側がこの決定を直接行うこともできるが、別のエンティティ（「識別交付者」または「識別サーバ」）がこのような識別とプラットフォームセキュリティとを証明する証明書を交付するようにして、ライセンス供与側は単にこの証明書に依存するようにすることが有用な場合もある。しかし、継続的なコンテンツ制御は、詐称者または安全でないプラットフォームに対して交付しないという証明書に依存するので、この分離は、ライセンス供与側が識別証明書の交付者を信用することを暗黙的に必要とする。配布および権利管理プロセスにおいて分離することのできる他の形態は、ライセンスを交付できる状況を定義するエンティティが、ライセンスを実際に交付するエンティティとは異なる場合である。したがって、コンテンツを発行する場合、第1のエンティティが、ライセンス供与条件を指定する権利ラベルにデジタル署名し、第2のエンティティが、コンテンツの使用を許可するライセンスを実際に交付することができる。このタイプの分離もやはり、第1のエンティティが、指定の条件下でのみライセンスを交付するよう第2のエンティティを信用することを必要とする。

30

40

#### 【0005】

##### 【発明が解決しようとする課題】

以上の考察から、誰がどんな状況下で文書をライセンス供与できるかに関する実際的現実

50

対するライセンスを得ることができるかについての領域は、配布およびライセンス供与プロセスに関与する様々なサーバ間で信用を広げる（または抑える）ことによって拡張（または収縮）させることができる。

【0006】

本発明は、従来技術で実現されていない、信用を用いてコンテンツへのアクセスを制御する技法を提供する。

【0007】

本発明は、信用モデルを使用して、権利管理されるコンテンツがどのように、またどんな状況でライセンス供与されるかに影響を与えるシステムおよび方法を提供することを目的とする。

【0008】

【課題を解決するための手段】

本発明によるデジタル権利管理（DRM）システムは、コンテンツのライセンス供与を受けるエンティティのみがコンテンツを使用できるような形でコンテンツを発行する。DRM保護されるコンテンツは、暗号化され、次いで「署名済み権利ラベル」付きで発行される。署名済み権利ラベルは、とりわけ（a）コンテンツをどのように使用することができるか、誰にライセンス供与することができるかを定義する権利データ、（b）権利ラベルを交付したサーバの公開鍵によって（直接的または間接的に）暗号化された、コンテンツのための復号鍵、および（c）権利ラベルを交付したサーバのデジタル署名を含む。権利管理されるコンテンツを受け取る可能性を有する各エンティティ（例えば個人、会社部門、非営利団体など）は、そのエンティティの識別を定義する「エンティティ証明書」を取得する。エンティティ証明書は（a）公開／秘密鍵の対、および（b）エンティティ証明書を交付したサーバの署名を含む。

【0009】

コンテンツをライセンス供与するよう求める要求は、コンテンツについての署名済み権利ラベルと、ライセンスの交付を受けるエンティティのエンティティ証明書とを含む。DRMライセンスサーバがこのような要求を受け取ると、DRMライセンスサーバは、ライセンス供与側が信用するサーバによってこのエンティティ証明書が署名されたことを決定する。（ライセンス供与側は例えば、サーバがこのような証明書を交付する前にエンティティの識別を十分厳格に検証すること、確認したい場合もある。）ライセンスサーバがエンティティ証明書の署名者を信用する場合、ライセンスサーバは、権利ラベルに署名したエンティティに代わってライセンスを交付できるかどうかを決定する。一般にライセンスサーバは、（a）サーバ自体が交付した権利ラベルと、（b）秘密鍵をライセンスサーバと共有していた他のDRMサーバとに基づいて、ライセンスを交付することができる。（権利ラベルは交付者サーバの公開鍵で暗号化されたコンテンツ復号鍵を含むので、ライセンスサーバは、権利ラベルを交付したサーバの秘密鍵を必要とする。ライセンスはエンティティ証明書の公開鍵で暗号化されたコンテンツ復号鍵を含むので、ライセンスサーバは、コンテンツ鍵をエンティティ証明書の公開鍵で再暗号化できるように、コンテンツ鍵を復号するための適用可能な秘密鍵を必要とする。）

DRMサーバのオペレータは、他のどのサーバが信用され、どのサーバが信用されないかを決定することにより、コンテンツをライセンス供与できる人々の領域を拡大（または縮小）することができる、さもないれば配布スキームのトポロジに影響を与えることができる。これらの決定は、様々な例示的な信用モデルとの関連で用いることができる。

【0010】

第1の例では、信用決定を利用して「信用ベルソナ領域」を実装することができ、DRMサーバが、エンティティ証明書を交付するものとして信用されるサーバのリストを維持する。このスキームは、2つの組織が、権利管理される情報をそれらのメンバーによって共有できるようにしたい場合に有用である。したがって、会社Aおよび会社Bがそれぞれ自社の従業員についてのエンティティ証明書を交付する場合、これらの会社は、相互の識別サーバを信用することに同意する。これにより、会社Aの従業員は、会社Bの従業員にライ

10

20

30

40

50

センス供与可能なコンテンツを発行することができ、その逆も可能である。会社Aの従業員によって発行されたコンテンツを受け取る会社Bの従業員は、権利ラベルおよび自分のエンティティ証明書会社AのDRMライセンスサーバに提示する。2つの会社は相互の識別サーバを信用することに同意しているため、このライセンスサーバは、会社Bの従業員のエンティティ証明書に対してコンテンツをライセンス供与することができる。この例の一変形は、DRMライセンスサーバが、eメールアドレスに基づく公用の識別サーバ(MICROSOFT.NET PASSPORTサーバなど)を一般に信用し、例外として、このようなサーバが特定のベルソナ(例えばjoe@untraceableaddress.com)またはドメイン(例えばuntraceableaddress.comからのすべてのアドレス)に交付した証明書は除くものである。さらにより一般的には、信用ベルソナ領域にある任意の識別サーバについて、eメールアドレス、ドメイン、または他の何らかの識別子に基づく除外リストを生み出すことができ、それによりライセンスサーバは、識別サーバを一般に信用すると共に、その信用に対する特定の例外を切り出すことができる。

10

#### 【0011】

第2の例では、信用決定を利用して「信用文書領域」を実装することができる。この場合、第1のDRMサーバが、第2のDRMサーバによって生み出された権利ラベルに基づいて、第2のDRMサーバの秘密鍵を得ることによってライセンスを交付することができる。実際このようなトランザクションは、第2のDRMサーバが、第2のサーバの代わりにライセンスを交付するものとして第1のDRMサーバを信用することを意味する。このスキームは、会社内の2つの部門がそれぞれDRMサーバを維持する場合(例えば2つの部門が地理的に離れている場合)に有用である。この場合、各部門は、他方の部門がそれ自体のDRMサーバ上でライセンス供与することのできるコンテンツを発行したいことがある。例えば、部門Aの従業員が部門AのDRMサーバを使用してコンテンツを発行し、発行したコンテンツを署名済み権利ラベルと共に部門Bの従業員に送る。次いで、部門Bの従業員は、ライセンスを求めて署名済み権利ラベルを部門BのDRMサーバにサブミットする。このシナリオは、部門Aの秘密鍵を部門BのDRMサーバに提供することによって可能にすることができる。

20

#### 【0012】

本発明のその他の特徴については以下に説明する。

30

#### 【0013】

以上の概要、ならびに後続の好適実施形態の詳細な説明は、添付の図面と共に読めはよりよく理解される。図面には、本発明を例示するために本発明の例示的な構造を示す。ただし本発明は、開示する特定の方法及び手段に限定されるものではない。

#### 【0014】

##### 【発明の実施の形態】

例示的なコンピューティング環境

図1および後続の考察に、本発明を実施することのできる適したコンピューティング環境の簡単な一般的記述を提供する。ただし、ハンドヘルド、ポータブル、およびその他あらゆる種類のコンピューティングデバイスが、本発明に関連した使用に企図されることを理解されたい。以下では汎用コンピュータについて説明するが、これは一例に過ぎず、本発明は、ネットワークサーバ相互運用性および対話を有するシンクライアントだけを必要とする。したがって本発明は、極めて少ないまたは最小限のクライアントリソースが関係する、ネットワークによってホストされるサービスの環境で実施することができる。例えば、クライアントデバイスが単にワールドワイドウェブに対するブラウザまたはインタフェースとして機能するだけのネットワーク化環境でも実施することができる。

40

#### 【0015】

必須ではないが本発明は、開発者が使用するためのアプリケーションプログラミングインタフェース(API)を介して実施することができ、および/または、ネットワーク閲覧ソフトウェアに含めることができる。これらについて、クライアントワークステーション

50



、サーバ、その他のデバイスなど、1つまたは複数のコンピュータによって実行されるプログラムモジュールなどのコンピュータ実行可能命令の一般的なコンテキストで説明する。一般にプログラムモジュールは、特定のタスクを実施するか特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。通常、プログラムモジュールの機能は、様々な実施形態で望むように組み合わせるが分散させることができる。さらに、本発明は他のコンピュータシステム構成で実施することもできることは、当業者なら理解するであろう。本発明と共に使用するのに適する他の周知のコンピューティングシステム、環境、および/または構成には、限定しないがパーソナルコンピュータ（PC）、現金自動預け払い機、サーバコンピュータ、ハンドヘルドデバイスまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、プログラム可能な民生用電子機器、ネットワークPC、ミニコンピュータ、メインフレームコンピュータなどが含まれる。本発明はまた、通信ネットワークまたはその他のデータ伝送媒体を介してリンクされたリモート処理デバイスによってタスクが実施される分散コンピューティング環境で実施することもできる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶デバイスを含めたローカルとリモートの両方のコンピュータ記憶媒体に位置することができる。

#### 【0016】

したがって図1に、本発明を実施することのできる適したコンピューティングシステム環境100の例を示す。ただし先に明確にしたように、コンピューティングシステム環境100は、適したコンピューティング環境の一例に過ぎず、本発明の使用または機能の範囲についてどんな制限を意味するものでもない。またコンピューティング環境100は、この例示的な動作環境100に示すコンポーネントのいずれか1つまたは組合せに関してどんな依存も要件も有するものと解釈すべきではない。

#### 【0017】

図1を参照すると、本発明を実施するための例示的なシステムは、コンピュータ110の形をとる汎用コンピューティングデバイスを含む。コンピュータ110のコンポーネントには、限定しないが処理ユニット120と、システムメモリ130と、システムメモリを含めた様々なシステムコンポーネントを処理ユニット120に結合するシステムバス121とを含めることができる。システムバス121は、様々なバスアーキテクチャのいずれかを用いた、メモリバスまたはメモリコントローラ、周辺バス、ローカルバスを含めて、いくつかのタイプのバス構造のいずれかとすることができる。限定ではなく例として、このようなアーキテクチャには、ISA（Industry Standard Architecture）バス、MCA（Micro Channel Architecture）バス、EISA（Enhanced ISA）バス、VESA（Video Electronics Standards Association）ローカルバス、およびPCI（Peripheral Component Interconnect）バス（メザンバスとも呼ばれる）が含まれる。

#### 【0018】

コンピュータ110は通常、様々なコンピュータ可読媒体を備える。コンピュータ可読媒体は、コンピュータ110からアクセスできる任意の利用可能な媒体とすることができ、揮発性と不揮発性、取外し可能と取外し不可能の両方の媒体が含まれる。限定ではなく例として、コンピュータ可読媒体には、コンピュータ記憶媒体および通信媒体を含めることができる。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、その他のデータなどの情報を記憶するための任意の方法または技術で実現される、揮発性と不揮発性、取外し可能と取外し不可能の両方の媒体が含まれる。コンピュータ記憶媒体には、限定しないがRAM、ROM、EEPROM、フラッシュメモリまたは他のメモリ技術、CD-ROM、デジタル多用途ディスク（DVD）または他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイスが含まれ、あるいは、所望の情報を記憶するのに使用できコンピュータ110からアクセスできるその他の任意の媒体が含まれる。通信媒体は通常、搬送波やその他のト

10

20

30

40

50

ランスポート機構など変調されたデータ信号中に、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを組み入れたものであり、任意の情報送達媒体が含まれる。「変調されたデータ信号」という語は、信号中の情報が符号化される形で1つまたは複数の特性が設定されたまたは変更された信号を意味する。限定ではなく例として、通信媒体には、配線式ネットワークや直接配線式接続などの配線式媒体と、音響、無線周波、赤外線、その他の無線媒体などの無線媒体とが含まれる。以上の任意の組合せもコンピュータ可読媒体の範囲に含めるべきである。

#### 【0019】

システムメモリ130は、読出し専用メモリ(ROM)131やランダムアクセスメモリ(RAM)132など、揮発性および/または不揮発性メモリの形のコンピュータ記憶媒体を含む。ROM131には通常、起動中などにコンピュータ110内の要素間で情報を転送するのに役立つ基本ルーチンを含むBIOS(basic input/output system)133が記憶されている。RAM132は通常、処理ユニット120がすぐにアクセス可能な、および/または処理ユニット120が現在作用している、データおよび/またはプログラムモジュールを含む。限定ではなく例として、図1には、オペレーティングシステム134、アプリケーションプログラム135、その他のプログラムモジュール136、およびプログラムデータ137を示す。

#### 【0020】

コンピュータ110は、その他の取外し可能/取外し不可能、揮発性/不揮発性コンピュータ記憶媒体を備えることもできる。例に過ぎないが図1には、取外し不可能および不揮発性の磁気媒体に対して読み書きするハードディスクドライブ141と、取外し可能および不揮発性の磁気ディスク152に対して読み書きする磁気ディスクドライブ151と、CD-ROMや他の光媒体など取外し可能および不揮発性の光ディスク156に対して読み書きする光ディスクドライブ155を示す。この例示的な動作環境で使用できる他の取外し可能/取外し不可能、揮発性/不揮発性コンピュータ記憶媒体には、限定しないが磁気テープカセット、フラッシュメモ리카ード、デジタル多用途ディスク、デジタルビデオテープ、固体RAM、固体ROMなどが含まれる。ハードディスクドライブ141は通常、インタフェース140などの取外し可能なメモリインタフェースを介してシステムバス121に接続され、磁気ディスクドライブ151および光ディスクドライブ155は通常、インタフェース150などの取外し可能メモリインタフェースでシステムバス121に接続される。

#### 【0021】

上述の図1に示した各ドライブおよびそれらに関連するコンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびその他のデータの記憶域をコンピュータ110に提供する。例えば図1には、ハードディスクドライブ141がオペレーティングシステム144、アプリケーションプログラム145、その他のプログラムモジュール146、およびプログラムデータ147を記憶しているのが示されている。これらのコンポーネントは、オペレーティングシステム134、アプリケーションプログラム135、その他のプログラムモジュール136、およびプログラムデータ137と同じものとするのもでき、異なるものとするのもできることに留意されたい。ここでは、オペレーティングシステム144、アプリケーションプログラム145、その他のプログラムモジュール146、およびプログラムデータ147が少なくとも異なるコピーであることを示すために、異なる番号を付してある。ユーザは、キーボード162や、マウス、トラックボール、またはタッチパッドと一般に呼ばれるポインティングデバイス161などの入力デバイスを介して、コンピュータ110にコマンドおよび情報を入力することができる。その他の入力デバイス(図示せず)には、マイクロホン、ジョイスティック、ゲームパッド、衛星受信アンテナ、スキャナなどを含めることができる。これらおよび他の入力デバイスは、システムバス121に結合されたユーザ入力インタフェース160を介して処理ユニット120に接続されることが多いが、パラレルポート、ゲームポート、ユニバーサルシリアルバス(「USB」)など、他のインタフェースおよびバス構造で接続

10

20

30

40

50

されてもよい。

#### 【0022】

モニタ191または他のタイプの表示デバイスもまた、ビデオインタフェース190などのインタフェースを介してシステムバス121に接続される。ノースブリッジなどのグラフィックスインタフェース182をシステムバス121に接続することもできる。ノースブリッジは、CPUまたはホスト処理ユニット120と通信し、AGP (accelerated graphics port) 通信に対する役割を担うチップセットである。1つまたは複数のグラフィックス処理ユニット (GPU) 184が、グラフィックスインタフェース182と通信することができる。なお、GPU 184は、一般にレジスタ記憶域などのオンチップメモリ記憶域を含み、ビデオメモリ186と通信する。ただし、GPU 184はコプロセッサの一例に過ぎず、したがって様々なコプロセッシングデバイスをコンピュータ110に含めることができる。モニタ191または他のタイプの表示デバイスもまた、ビデオインタフェース190などのインタフェースを介してシステムバス121に接続され、ビデオインタフェース190はビデオメモリ186と通信することができる。モニタ191に加えて、コンピュータは通常、スピーカ197やプリンタ196など他の周辺出力デバイスも備えることができ、これらは出力周辺インタフェース195を介して接続することができる。

#### 【0023】

コンピュータ110は、リモートコンピュータ180など1つまたは複数のリモートコンピュータへの論理接続を用いて、ネットワーク化された環境で動作することができる。リモートコンピュータ180は、パーソナルコンピュータ、サーバ、ルータ、ネットワークPC、ピアデバイス、または他の一般的なネットワークノードとすることができ、図1にはメモリ記憶デバイス181しか示していないが、通常はコンピュータ110に関して上述した要素の多くまたはすべてを備える。図1に示す論理接続は、ローカルエリアネットワーク (LAN) 171およびワイドエリアネットワーク (WAN) 173を含むが、他のネットワークを含むこともできる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、およびインターネットでよくみられるものである。

#### 【0024】

コンピュータ110は、LANネットワーキング環境で使用される場合、ネットワークインタフェースまたはアダプタ170を介してLAN 171に接続される。WANネットワーキング環境で使用される場合は通常、インターネットなどのWAN 173を介した通信を確立するためのモデム172または他の手段を備える。モデム172は内蔵でも外付けでもよく、ユーザ入力インタフェース160または他の適切な機構を介してシステムバス121に接続することができる。ネットワーク化環境では、コンピュータ110に関して示したプログラムモジュールまたはその一部をリモートのメモリ記憶デバイスに記憶することができる。限定ではなく例として、図1には、リモートアプリケーションプログラム185がメモリデバイス181上にあるものとして示す。図示のネットワーク接続は例示的なものであり、コンピュータ間に通信リンクを確立する他の手段を使用することもできることは理解されるであらう。

#### 【0025】

デジタルコンテンツの発行

図2は、デジタルコンテンツを発行するための、本発明によるシステムおよび方法の好適実施形態の機能ブロック図である。本明細書において「発行」という語は、信用されるエンティティがこのコンテンツに対して交付できる権利および条件のセット、ならびにこれらの権利および条件を交付できる対象を、信用されるエンティティによって確立するために、アプリケーションまたはサービスが従うプロセスを指す。本発明によれば、発行プロセスは、デジタルコンテンツを暗号化し、可能性あるすべてのコンテンツユーザに向けてコンテンツの作者が意図した永続的および施行可能な権利のリストを関連付けることを含む。このプロセスは、コンテンツの作者が意図しない限りどんな権利またはコンテン

10

20

30

40

50

ツへのアクセスも禁じるように安全な方法で実施することができる。

【0026】

本発明の好適な実施形態では、特に3つのエンティティを利用して安全なデジタルコンテンツを発行することができる。すなわち、クライアント300上で実行され、発行に向けてコンテンツを作成するコンテンツ作成アプリケーション302と、やはりクライアントデバイス300上にあるデジタル権利管理(DRM)アプリケーションプログラムインタフェース(API)306と、通信ネットワーク330を介してクライアント300と通信可能に結合されたDRMサーバ320である。本発明の好適な実施形態では、通信ネットワーク330にはインターネットが含まれるが、通信ネットワーク330は、例えばプロプライエタリイントラネットなど、任意のローカルまたはワイドエリアネットワークとすることができることを理解されたい。

10

【0027】

コンテンツ作成アプリケーション302は、デジタルコンテンツを生成する任意のアプリケーションとすることができる。例えばアプリケーション302は、ワードプロセッサとすることができる。あるいは、デジタルテキストファイル、デジタル音楽、ビデオ、または他のそのようなコンテンツを生成するその他の発行側とすることができる。コンテンツには、例えばライブイベントまたはテープに記録されたイベントのストリーミングオーディオ/ビデオなど、ストリーミングコンテンツを含めることもできる。本発明によれば、コンテンツ作成アプリケーションは、そのユーザに、ユーザの提供する鍵(CK)を使用してコンテンツを暗号化するように促す。アプリケーション302は、この鍵を使用してデジタルコンテンツを暗号化し、それにより暗号化済みデジタルコンテンツファイル304を形成する。クライアントアプリケーションはまた、デジタルコンテンツファイル304に対する権利を提供するようユーザに促す。権利データは、デジタルコンテンツにおける権利を有する各エンティティの識別を含む。このようなエンティティは、例えば、個人、ある部類の複数の個人、またはデバイスとすることができる。このような各エンティティについて、権利データはまた、コンテンツにおいてそのエンティティが有する権利、およびこれらの権利のいずれかまたはすべてに課すことのできる条件のリストも含む。このような権利には、デジタルコンテンツの読出し、編集、コピー、印刷などの権利を含めることができる。さらに、権利は包含的とすることも排他的とすることもできる。包含的な権利は、指定のユーザがコンテンツにおいて指定の権利を有することを示す(例えばこのユーザはデジタルコンテンツを編集することができる)。排他的な権利は、指定のユーザがコンテンツにおいて指定の権利を除くすべての権利を有することを示す(例えばこのユーザは、コピーすることを出ては、デジタルコンテンツで何をしてもよい)。

20

30

【0028】

本発明の一実施形態によれば、クライアントAPI306は、暗号化済みデジタルコンテンツおよび権利データをDRMサーバ320に渡すことができる。DRMサーバ320は、以下に詳細に説明するプロセスを用いて、ユーザから譲渡された権利を施行することができるかどうかを決定し、施行することができる場合は、権利データに署名して、署名済み権利ラベル(SRL)308を形成する。ただし一般には、信用される任意のエンティティが、好ましくはDRMサーバ320によって信用される鍵を使用して、権利データに署名することができる。例えば、クライアントが、DRMサーバ320から提供された鍵を使用して権利データに署名することができる。

40

【0029】

権利ラベル308は、権利記述と、暗号化済みコンテンツ鍵と、権利記述および暗号化済みコンテンツ鍵に対するデジタル署名とを表すデータを含むことができる。DRMサーバが権利ラベルに署名していれば、DRMサーバは、クライアントAPI306を介して署名済み権利ラベル308をクライアントに返し、クライアントは、署名済み権利ラベル308をクライアントデバイス300上に記憶する。次いで、コンテンツ作成アプリケーション302は、署名済み権利ラベル308を暗号化済みデジタルコンテンツファイル

50

304と関連付ける。例えば、SRL308を暗号化済みデジタルコンテンツファイルと連結して、権利管理されるコンテンツファイル310を形成することができる。ただし一般に、権利データはデジタルコンテンツと結合しなくてもよい。例えば、権利データを既知の位置に記憶し、記憶した権利データへの参照を暗号化済みデジタルコンテンツと結合してもよい。この参照は、この権利データがどこに記憶されているかを示す識別子（例えばこの権利データを含むデータ記憶域）、および、特定の記憶位置にあるこの特定の権利データに対応する識別子（例えば当該の特定の権利データを含むファイルを識別する識別子）を含むことができる。この場合、権利管理コンテンツ310は、どこにいる誰にでも送達することができ、コンテンツを消費する権利を有するエンティティだけが、譲渡された権利に従ってのみコンテンツを消費することができる。

10

#### 【0030】

SRL308はデジタル署名された文書であり、これにより改ざんできないようになっている。さらに、SRL308は、コンテンツの暗号化に使用される実際の鍵タイプおよびアルゴリズムからは独立しているが、それが保護するコンテンツとの強力な1対1関係を維持する。ここで図3を参照するが、本発明の一実施形態で、SRL308は、コンテンツに関する情報を含むことができる。これはSRL308の基礎であり、おそらくコンテンツのIDを含む。SRL308はさらに、SRL308に署名するDRMサーバに関する情報を含む。これは(PU-DRM(DES1))と、ネットワーク上でDRMサーバを突き止めるためのURLや、URLが失敗した場合のフォールバック情報などの参照情報とを含む。さらに、SRL308はとりわけ、SRL308自体を記述する情報、(DES1(権利データ))、(DES1(CK))、およびS(PR-DRM)を含む。

20

#### 【0031】

信用されるエンティティが権利データに署名して署名済み権利ラベル308を生み出すことを確実にすることにより、DRMサーバは、権利ラベル308の権利データに記述されるように発行元によって示される条件に従ってコンテンツに対するライセンスを交付することを表明する。理解されるはずだが、ライセンスはコンテンツ鍵(CK)を含むので、特にユーザは、コンテンツを提供するライセンスを得る必要がある。ユーザは、暗号化済みコンテンツに対するライセンスを得たい場合、コンテンツについてのSRL308と、ユーザの資格を証明する証明書とを含むライセンス要求を、DRMサーバ320またはその他のライセンス交付エンティティに提示することができる。次いでライセンス交付エンティティは、(PU-DRM(DES1))および(DES1(権利データ))を復号して権利データを生成し、作者(もしあれば)からライセンス要求元エンティティに供与されるすべての権利をリストし、これらの特定の権利だけを含むライセンスを構築することができる。

30

#### 【0032】

アプリケーション302がSRL308を受け取ったとき、このようなアプリケーション302は、署名済み権利ラベル308に対応する(CK(内容))304と連結して、権利管理されるデジタルコンテンツを形成することが好ましい。代わりに、権利データを既知の位置に記憶し、この位置への参照を暗号化済みデジタルコンテンツと共に提供してもよい。これにより、DRM対応の提供アプリケーションが、提供しようとするコンテンツを介して署名済み権利ラベル308を発見することができる。この発見により、提供アプリケーションがトリガされて、DRMライセンス供与サーバ320に対するライセンス要求が開始する。発行アプリケーション302は、例えばDRMライセンス供与サーバ320へのURLを記憶することができる。あるいは、DRMライセンス供与サーバ320は、権利ラベルにデジタル署名する前にそれ自体のURLをメタデータとして権利ラベルに組み込み、提供アプリケーションから呼び出されたDRMクライアントAPI306が正しいDRMサーバ320を識別できるようにすることもできる。権利ラベルに署名する前に、固有の識別子、例えばGUID(9106a11x unique identifier)などを挿入することが好ましい。

40

#### 【0033】

50

本発明の好適な実施形態では、コンテンツ作成アプリケーション302または提供アプリケーションと、DRMサーバ320との間の通信には、SOAP(Simple Object Access Protocol)を使用することができる。さらに、DRMプロトコルのクライアント側を実装するのにアプリケーション302などのアプリケーションを必要とするのではなくローカルAPI呼出しを行うだけでよいように、API306などのAPIライブラリを設けることができる。デジタルコンテンツについての権利記述、ライセンス、および権利ラベルを記述するためには、XML言語であるXMLを使用することが好ましいが、権利記述およびその他のデータには、適した任意のフォーマットを使用することができることを理解されたい。

#### 【0084】

発行されたコンテンツに対するライセンスの取得

図4は、権利管理されるデジタルコンテンツをライセンス供与するための、本発明によるシステムおよび方法の好適実施形態の機能ブロック図である。本明細書において「ライセンス供与」という語は、ライセンス中で指名されたエンティティがライセンス中で指定された条件に従ってコンテンツを消費することを可能にするライセンスを要求し受け取るために、アプリケーションまたはサービスが従うプロセスを指す。ライセンス供与プロセスへの入力には、ライセンス要求されているコンテンツに関連する署名済み権利ラベル(SRL)308と、ライセンス要求が行われているエンティティの公開鍵証明書を含めることができる。ライセンスを要求しているエンティティは、必ずしもライセンス要求が行われているエンティティであるとは限らないことに留意されたい。通常、ライセンスは、SRL308からの権利記述と、暗号化済みコンテンツを復号することのできる暗号化済み鍵と、権利記述および暗号化済み鍵に対するライセンスサーバからのデジタル署名とを含む。デジタル署名は、指定されたエンティティおよび権利が正当であることを表明する。

#### 【0085】

アプリケーション302が権利管理コンテンツ310を消費する方法の1つは、クライアントAPI306が通信ネットワーク330を介して権利管理コンテンツ310の署名済み権利ラベル308をDRMサーバ320に転送するものである。DRMサーバ320の位置は、例えばSRL308中の参照情報中から知ることができる。このような実施形態では、DRMライセンス供与サーバ320は、後で詳述するプロセスによって、ライセンスを交付できるかどうかを権利ラベル中の権利記述を使用して決定することができる。交付できる場合は、権利記述を取り出してライセンスに含めることができる。前述のように、権利ラベル308は、DRMサーバ320の公開鍵(PU-DRM)に従って暗号化されたコンテンツ鍵(CK)(すなわちPU-DRM(CK))を含む。ライセンスを交付するプロセスにおいて、DRMサーバ320は、この値を安全に復号して(CK)を得る。次いで、ライセンス要求中で渡された公開鍵証明書中の公開鍵(PU-ENTITY)を使用して、(CK)を再暗号化する(すなわち(PU-ENTITY(CK)))。新たに暗号化されたこの(PU-ENTITY(CK))を、サーバ320はライセンス中に挿入する。したがって、関連する秘密鍵(PR-ENTITY)の保持者だけが(PU-ENTITY(CK))から(CK)を回復することができるので、(CK)を露出する危険なしにライセンスを呼出し元に返すことができる。次いで、クライアントAPI306は、(CK)を使用して暗号化済みコンテンツを復号し、復号されたデジタルコンテンツ312を形成する。次いで、クライアントアプリケーション302は、ライセンス中で提供される権利に従って、復号されたデジタルコンテンツ312を使用することができる。

#### 【0086】

別法として、例えば発行クライアントなどのクライアントが、コンテンツを消費するためのそれ自体のライセンスを交付することもできる。このような実施形態では、デジタルコンテンツを適切な状況で復号するのに必要な鍵をクライアントに提供する安全なプロセスを、クライアントコンピュータ上で実行することができる。

10

20

30

40

50

## 【0037】

図5Aおよび5Bに、権利管理されるデジタルコンテンツをライセンス供与するための、本発明による方法600の好適な実施形態のフローチャートを提供する。本発明によれば、要求エンティティが、1つまたは複数の潜在的ライセンス取得側に代わってライセンス要求をサブミットすることができる。要求エンティティは、潜在的ライセンス取得側の1つであっても、そうでなくてもよい。潜在的ライセンス取得側は、個人、グループ、デバイス、または、任意のスキームでコンテンツを消費することのできる任意のこのようなエンティティとすることができる。ここで、DRMサーバがライセンス要求を処理する一実施形態に関して方法600を説明するが、ライセンス要求の処理をクライアント上で実施し、クライアントがライセンスを交付することでもできることを理解されたい。

10

## 【0038】

ステップ602で、例えばDRMサーバなどのライセンス交付エンティティが、ライセンス要求を受け取る。ライセンス要求は、要求が行われている1つまたは複数のライセンス取得側それぞれについての公開鍵証明書と識別のどちらかを含むことが好ましい。

## 【0039】

ステップ604で、要求エンティティ（すなわちライセンス要求を行っているエンティティ）を認証する。本発明の一実施形態によれば、ライセンス交付エンティティは、プロトコル（例えばチャレンジャーレスポンス）認証を用いて要求エンティティの識別を決定するように構成することでもでき、あるいは、要求エンティティの認証を必要としないように構成することでもできる（「匿名認証を可能にする」とも言われる）。認証を必要とする場合は、任意のタイプの認証スキームを使用することができる（例えば前述のチャレンジャーレスポンススキームや、MICROSOFT、NET、PASSPORT、WINDOWS（登録商標）認証×509などのユーザIDおよびパスワードスキーム）。匿名認証を可能にし、および、統合情報システムによってサポートされる任意のプロトコル認証スキームをサポートすることが好ましい。認証ステップの結果は、例えば「匿名」識別（匿名認証の場合）や個人アカウント識別などの識別となる。何らかの理由でライセンス要求を認証することができない場合は、エラーを返し、ライセンスは供与しない。

20

## 【0040】

ステップ606で、認証された識別を許可する。すなわち、ステップ604で認証された識別が（それ自体でまたは別のエンティティの代わりに）ライセンスを要求することができるとかを決定する。ライセンス交付エンティティは、ライセンスを要求することが許可される（または許可されない）エンティティのリストを記憶していることが好ましい。好適な実施形態では、この識別リスト中の識別は、ライセンス要求が行われているエンティティの識別ではなく、要求を行っているエンティティの識別であることが好ましいが、このどちらでもよい。例えば、個人アカウント識別が直接にライセンス要求を行うことは許可されないが、信用されるサーバプロセスがこのようなエンティティに代わってライセンス要求を行うことはできるものとすることができる。

30

## 【0041】

本発明によれば、ライセンス要求は、潜在的ライセンス取得側それぞれについての公開鍵証明書と識別のどちらかを含むことができる。1つのライセンス取得側だけのためにライセンスが要求される場合は、1つの証明書または識別だけが指定される。複数のライセンス取得側のためにライセンスが要求される場合は、それぞれの潜在的ライセンス取得側について証明書または識別を指定することができる。

40

## 【0042】

ライセンス交付エンティティは、有効な各ライセンス取得側についての公開鍵証明書を有することが好ましい。しかし、アプリケーション302は、所与のユーザのためのライセンスを生成したいと思ってもこのユーザについての公開鍵証明書にアクセスできない場合がある。このような状況では、アプリケーション302は、このユーザの識別をライセンス要求中で指定することができる。この結果、ライセンス交付エンティティは登録済み証明書プラグインモジュールを呼び出すことができ、このプラグインモジュールは、ディレ

50



クトリサービスを検索して適切なユーザの公開鍵証明書を返す。

【0043】

ステップ608で、ライセンス要求に公開鍵証明書が含まれていないとライセンス交付エンティティが決定した場合、交付エンティティは、指定された識別を使用して、ディレクトリサービスまたはデータベース中で適切な公開鍵証明書を検索する。ステップ610で、証明書がディレクトリ中にあると交付エンティティが決定した場合は、ステップ612でこの証明書を取り出す。好適な実施形態では、証明書プラグインを使用して、ディレクトリアクセスプロトコルによって公開鍵証明書をディレクトリサービスから取り出す。所与の潜在的ライセンス取得側についての証明書が要求中にもディレクトリ中にも見つからない場合は、ライセンスサーバはこの潜在的ライセンス取得側に対してライセンスを生成せず、ステップ614で要求エンティティにエラーを返す。

10

【0044】

ライセンス交付エンティティが少なくとも1つの潜在的ライセンス取得側についての公開鍵証明書を有すると仮定すると、ステップ616で、交付エンティティはこのライセンス取得側の信用を妥当性検査する。好ましくは、交付エンティティは、信用される証明書交付者の証明書のセットを有するように構成され、信用される交付者のリスト中にライセンス取得側の証明書の交付者があるかどうかを決定する。ステップ616で、信用される交付者のリスト中にライセンス取得側の証明書の交付者がいないと交付エンティティが決定した場合は、このライセンス取得側についての要求は失敗し、ステップ614でエラーが生成される。したがって、信用される交付者によってその証明書が交付されていない潜在的

20

【0045】

さらに、交付エンティティは、信用される交付者の証明書から個々のライセンス取得側の公開鍵証明書までの証明書チェーン中のすべてのエンティティに対してデジタル署名の妥当性検査を行うことが好ましい。チェーン中でデジタル署名を妥当性検査するプロセスは、周知のアルゴリズムである。所与の潜在的ライセンス取得側についての公開鍵証明書の妥当性が認められない場合、またはチェーン中の証明書の妥当性が認められない場合は、この潜在的ライセンス取得側は信用されず、したがってこの潜在的ライセンス取得側にライセンスは交付されない。そうでない場合は、ステップ618でライセンスを交付することができ、このプロセスは、ステップ620で、ライセンス要求が行われているすべてのエンティティが処理されるまで繰り返す。

30

【0046】

図5Bに示すように、ライセンス交付エンティティは、ライセンス要求中で受け取った署名済み権利ラベル308の妥当性検査に進む。好適実施形態では、交付エンティティは、権利ラベルプラグインおよびバックエンドデータベースを使用して、交付エンティティが署名したあらゆる権利ラベルのマスタコピーをサーバ上に記憶することができ、権利ラベルは、発行時に挿入されたGUIDで識別される。ライセンス時（ステップ622）、交付エンティティは、ライセンス要求中の権利ラベル入力を解析し、そのGUIDを取り出す。次いでこのGUIDを権利ラベルプラグインに渡し、権利ラベルプラグインは、データベースに対する照会を発行して、マスタ権利ラベルのコピーを取り出す。マスタ権利ラベルは、ライセンス要求中で送られた権利ラベルのコピーよりも最新のものとすることができ、これが以下のステップにおいて要求中で使用される権利ラベルになる。権利ラベルがデータベース中でGUIDに基づいて見つからない場合は、ステップ624で、交付エンティティはそのポリシーをチェックして、要求中の権利ラベルに基づいてライセンスを交付することがまだ許可されるかどうかを決定する。ポリシーがこれを許可しない場合は、ステップ626でライセンス要求は失敗し、ステップ628でエラーがAPI306に返される。

40

【0047】

ステップ630で、ライセンス交付エンティティは権利ラベル308を妥当性検査する。権利ラベル上のデジタル署名を妥当性検査し、ライセンス交付エンティティが権利ラベ

50



ルの交付者（それに署名したエンティティ）でない場合は、ライセンス交付エンティティは、権利ラベルの交付者が別の信用されるエンティティ（例えばライセンス交付エンティティが鍵材料を共有できるようになっているエンティティ）がどうかを決定する。権利ラベルの妥当性が認められない場合、または信用できるエンティティによって交付されたものでない場合は、ステップ626でライセンス要求は失敗し、ステップ628でエラーがAPI306に返される。

#### 【0048】

すべての妥当性検査を行った後、ライセンス交付エンティティは、権利ラベル308を、承認された各ライセンス取得側に対するライセンスに変換する。ステップ632で、ライセンス交付エンティティは、各ライセンス取得側に交付するライセンスについて各権利記述を生成する。各ライセンス取得側につき、交付エンティティは、そのライセンス取得側の公開鍵証明書中で指定された識別を、権利ラベル中の権利記述中で指定された識別に対して評価する。権利記述は、あらゆる権利または権利セットに、ライセンス中の、その権利または権利セットを実施することのできる識別のセットを割り当てる。このライセンス取得側の識別が関連するあらゆる権利または権利セットにつき、その権利または権利セットが、このライセンスについての新しいデータ構造中にコピーされる。得られるデータ構造が、この特定のライセンス取得側に対するライセンス中の権利記述である。このプロセスの一部として、ライセンス交付エンティティは、権利ラベルの権利記述中のいずれかの権利または権利セットと関連するかもしれない前提条件があればそれを評価する。例えば、ある権利には、ライセンス交付エンティティが指定時間以後にライセンスを交付することを制限する時間前提条件が関連するものとすることができる。この場合、交付エンティティは現在時間をチェックする必要がある。前提条件に指定された時間を過ぎていれば、交付エンティティは、ライセンス取得側の識別がその権利に関連していても、このライセンス取得側に権利を交付することはできない。

#### 【0049】

ステップ636で、交付エンティティは、（P U - D R M（D E S 1））および（D E S 1（C K））を権利ラベル308からとり、（P R - D R M）を適用して（C K）を得る。次いで交付エンティティは、（P U - E N T I T Y）すなわちライセンス取得側の公開鍵証明書を使用して（C K）を再暗号化し、その結果（P U - E N T I T Y（C K））を得る。ステップ638で、交付エンティティは、生成した権利記述を（P U - E N T I T Y（C K））と連結し、得られたデータ構造に（P R - D R M）を使用してデジタル署名する。この署名済みデータ構造が、この特定のライセンス取得側エンティティに対するライセンスである。

#### 【0050】

ステップ640で、特定の要求について生成するライセンスがそれ以上ないと交付エンティティが決定したとき、交付エンティティは0個またはそれ以上のライセンスを生成したことになる。ステップ642で、生成したライセンスを、これらのライセンスに関連する証明書チェーン（例えば、サーバ自体の公開鍵証明書、ならびにその証明書を交付した証明書など）と共に要求エンティティに返す。

#### 【0051】

本発明によるシステムの好適な実施形態では、ライセンス供与側の鍵を複数使用することができる。このような実施形態では、暗号化されて権利ラベル308を通りライセンス中に入るコンテンツ鍵（C K）は、実際、任意のどんなデータとすることもできる。特に有用な一変形は、暗号化された別個のコンテンツ鍵（C K）を複数使用するものであり、コンテンツ鍵（C K）はそれぞれ、権利記述中の異なる権利または異なる当人に関連する。例えば、アルバムの中の歌のデジタルバージョンをすべて異なる鍵（C K）で暗号化することができる。これらの鍵（C K）は、同じ権利ラベル中に含まれることになるが、ある当人は、これらの歌のうちの1つを再生する権利を有することができる（例えば、彼は自分のライセンス中で1つの鍵を得る権利しか有さない）、第2の当人は、すべての歌を再生する権利を有する（彼女は自分のライセンス中ですべての鍵を得る権利を有する）。

10

20

30

40

50

## 【0052】

本発明によるシステムでは、発行アプリケーション/ユーザが、ライセンス取得側のグループまたは種類を権利ラベル308中で指定できることが好ましい。このような実施形態では、ライセンス交付エンティティは、権利ラベル中で指定されたどんなグループ/種類も評価して、現在のライセンス取得側の識別がこれらのグループまたは種類のメンバーであるかどうかを決定する。指定されたグループ/種類中のメンバシップが見つかった場合は、交付エンティティは、このグループ/種類に関連する権利または権利セットを、ライセンスに使用される権利記述データ構造に加えることができる。

## 【0053】

本発明の好適な実施形態では、DRMサーバ中の発行プロトコルインタフェースおよびライセンスプロトコルインタフェースが、呼出し側アプリケーションまたはユーザの認証および許可をサポートし、DRMサーバのための管理コンソールにより、管理者は、ライセンス供与インタフェースと発行インタフェースの両方についてのアクセス制御リストを生成することができる。これにより、サーバの顧客は、どのユーザ/アプリケーションが発行またはライセンス供与、あるいはその両方を行うことができるかに関するポリシーを適用することができる。

## 【0054】

例示的なプラットフォーム、ならびにこれと識別およびライセンスとの関係  
本発明がサポートする信用モデルは、権利管理されるコンテンツの保護が、コンテンツを保護する鍵の保護に依存するという考えに基づく。先に論じたように、コンテンツは、ユーザの提供する対称鍵CKで暗号化される。コンテンツの最終的な消費者はコンテンツを復号するためにCKを必要とするので、DRMシステムが解決しなければならない問題の1つは、鍵が移送中に見られないように、およびコンテンツ消費者が鍵を濫用しないように、どのようにして鍵を安全なスキームで消費者に提供するかである。図6〜8に、鍵CKを安全なスキームでユーザに提供するために使用することのできる構造を示す。

## 【0055】

図6には、暗号サービスを提供する例示的なプラットフォーム602を示す。プラットフォーム602は、公開/秘密鍵の対であるP U - P L A T F O R M / P R - P L A T F O R Mと、この鍵の対を適用して暗号サービスを実施する暗号モジュール604を含む。プラットフォーム602の機能は、秘密のプラットフォーム鍵P R - P L A T F O R Mを明かすずにこれらの暗号サービスを実施することである。したがって、プラットフォーム602を利用するオブジェクトは、暗号要求（例えばコンテンツを復号する要求や、デジタル署名を検証する要求）を提供し、暗号結果（例えば復号されたコンテンツや署名検証）を受け取る。プラットフォーム602は、秘密のプラットフォーム鍵P R - P L A T F O R Mをユーザに明かすずに結果を提供するので、「ブラックボックス」と呼ばれることもある。

## 【0056】

プラットフォーム602は様々な実装形態を有することができるが、本発明によりこれらの実装形態のいずれを使用することもできる。例えばプラットフォーム602は、改ざん防止が施されたソフトウェアのようなものとすることができ、秘密プラットフォーム鍵を隠された形で含み、コード難読化技法を用いて、ハッカーがソフトウェアを分析することによって秘密鍵を知ろうとするのを困難にする。別の例として、プラットフォーム602は自己完結型の集積回路とすることができ、分析を受けないよう回路を保護する、および/または防壁侵入が試みられた場合に回路を自己破壊させる、物理防壁が付いたものとすることができる。権利管理されるコンテンツがコンピュータ上で使用可能な場合に、各コンピュータは、固有の鍵の対を備えたこのようなプラットフォームを1つ有することが期待される。秘密鍵を保護するのに使用される手段にかかわらず、前述の暗号機能を実施する任意のプラットフォームを本発明により使用することができる。ただし、図9に関連して後述するが、秘密鍵の保護に使用される手段はプラットフォームの信用に影響する。

## 【0057】

10

20

30

40

50

図 7 に、例示的な識別証明書 702 を示す。識別証明書 702 は、ペルソナについての識別を定義する。この場合、人物は john@microsoft.com であり、したがって、john@microsoft.com が権利管理コンテンツに対するライセンスを得たいときは、識別証明書 702 が、このライセンスを作成することになる DRM サーバに対して john@microsoft.com が自分を識別するのに使用するデータ構造である。識別証明書 702 は、公開鍵 P U - E N T I T Y についての公開鍵証明書と、プラットフォームの公開鍵 P U - P L A T F O R M で暗号化された秘密鍵 P R - E N T I T Y と、識別証明書 702 の交付者のデジタル署名（この交付者の秘密鍵 P R - I S S U E R を使用して生み出される）とを含む。

【0058】

図 4、5A、5B に関連して先に論じたように、ライセンス要求中、P U - E N T I T Y を含む証明書が DRM サーバに渡される。識別証明書 702 は、このような証明書の例である。したがって P U - E N T I T Y は、ステップ 636（図 5B に示す）でコンテンツ鍵 C K を暗号化するのに使用される鍵である。識別証明書 702 はユーザのマシンにインストールされることになるので、ユーザが P R - E N T I T Y への直接アクセスを有さないことが重要である。というのは、P R - E N T I T Y を有する者は誰でもライセンス中のコンテンツ鍵 C K を復号してコンテンツの保護を損なうことができるからである。このため、プラットフォーム 602 がライセンスから C K を復号するために P R - E N T I T Y が必要になったときに P R - E N T I T Y を復号することができるように、識別証明書 702 は、P U - P L A T F O R M で暗号化された P R - E N T I T Y を記憶している。P R - E N T I T Y を有する者は誰でもコンテンツを盗む力を持つので、識別証明書 702 中のデジタル署名は、P R - E N T I T Y が保護されており、安全でないプラットフォームに配布されていないという、証明書交付者の保証を表す。

【0059】

識別証明書 702 は、ユーザのコンピュータをユーザの識別から分離することをサポートすることに留意されたい。したがって、john@microsoft.com は、複数のプラットフォーム用に証明書が再作成されるようにするだけで、自分の識別が複数のコンピュータにインストールされるようにすることができる（同じ識別に対して交付できる証明書の数、またはこのような証明書をインストールできるプラットフォームのタイプを制限する識別プラットフォームがある場合もある）。これらの様々な証明書は、証明書中の P R - E N T I T Y を暗号化する公開鍵 P U - P L A T F O R M がプラットフォームごとに異なることを除いては同じとなる。さらに、識別証明書 702 はグループ識別を生み出すこともサポートする。例えば、自動車会社の自動車部品部門が識別を有することができる。これにより、自動車部品部門にいる全員のコンピュータに自動車部品識別証明書がインストールされるようにするだけで、自動車部品部門の全体に文書をライセンス供与することができる、および消費可能にすることができる。

【0060】

図 8 に、識別に交付されるライセンス 802 を示す。ライセンス 802 は、権利（すなわち、コンテンツで何ができるか、およびコンテンツを消費することのできる状況を律する規則）と、P U - E N T I T Y によって暗号化されたコンテンツ鍵 C K と、ライセンスを交付した DRM サーバの秘密鍵 P R - D R M を使用して生み出された署名を含む。図 8 でわかるように、C K は、秘密の識別鍵 P R - E N T I T Y を使用して P U - E N T I T Y （C K）を復号することによってのみ、ライセンスから回復することができる。したがって、これがライセンスから C K を回復する唯一の方法なので、実際、ライセンスを使用するには P R - E N T I T Y を含む識別証明書 702 がなければならない。さらに、識別証明書 702 中の P R - E N T I T Y は公開プラットフォーム鍵 P U - P L A T F O R M で暗号化されるので、識別証明書は、コンテンツが消費されるプラットフォーム 602 用に限定して生み出されなければならない。このため、ライセンスを使用してコンテンツを消費するには、ユーザには、自分の識別に交付されたライセンスと、コンテンツが消費されるプラットフォームに交付された識別証明書がなければならない。

## 【0061】

## 信用のモデル

前述のDRMシステムは、複数の鍵の層を介してコンテンツを保護する。これらの鍵の層は、コンテンツ所有者からコンテンツが最終的に使用されるプラットフォームに至る信用関係のチェーンを表す。図9に、様々な鍵の間の関係と、これらの鍵が意味する信用のチェーンを示す。

## 【0062】

図9に示すように、コンテンツ902は、コンテンツ鍵904（前の考察でCKと呼んでいた）で保護される。コンテンツ鍵904は、識別鍵の対906（PU-ENTITTY/PR-ENTITTY）で保護される。秘密の識別鍵は、プラットフォーム鍵の対908（PU-PLATFORM, PR-PLATFORM）で保護される。先に論じたように、秘密の識別鍵（PR-ENTITTY）は、コンピューティングデバイス上で識別証明書内に記憶されて、コンピューティングデバイスの公開プラットフォーム鍵で、すなわちPU-PLATFORM（PR-ENTITTY）として暗号化されることが好ましい。これにより、PR-ENTITTYはPR-PLATFORMでしか復号することができない。

## 【0063】

コンテンツ902からプラットフォーム鍵の対908までの保護チェーンにおけるどんな脆弱性も、コンテンツ902のセキュリティを脅かすことは容易に理解されるであろう。したがって、コンテンツ鍵904が公に知られた場合、誰でもコンテンツ902を復号することができる。同様に、秘密の識別鍵が公に知られた場合、誰でもコンテンツ鍵904を復号することができ、次にコンテンツ902を復号することができる。最後に、秘密のプラットフォーム鍵が公に知られた場合、誰でも秘密の識別鍵を復号することができ、それによりコンテンツ鍵を復号することができ、それによりコンテンツを復号することができる。このため、これらの暗号化の層を介してコンテンツへのアクセスを与えることについてのセキュリティは、コンテンツ鍵、秘密の識別鍵、および秘密のプラットフォーム鍵が損なわれないことに依存する。

## 【0064】

したがって、保護すべきこれらの各鍵の機能は、信用のチェーンを介して確立される。このチェーンを図9の要素912から918に示す。コンテンツ所有者912は、コンテンツを発行するときにコンテンツ鍵CKを生み出し、この鍵を、署名のために権利ラベルが提示されるときにライセンス供与側（すなわちDRMサーバ）と共有する。したがって、コンテンツ所有者912は、コンテンツへの自由なアクセスを与えたくないのに、ライセンス供与側914がコンテンツ鍵を損なわないものと実質的に信用する。すなわち、制御された状況下でのみコンテンツ鍵を配布するものと信用する。同様に、ライセンス供与側は、特定の識別にライセンスを交付するとき（必然的に、秘密の識別鍵を使用してコンテンツ鍵を復号できるような形でコンテンツ鍵を分与することを含む）、秘密の識別鍵が適切な制御条件下でのみ使用できるように、識別証明書の交付者916が識別証明書を交付したことを本質的に信用する。証明書交付者916は、所与のプラットフォーム918に識別証明書を交付するとき（それによりプラットフォームが秘密の識別鍵PR-ENTITTYを使用できるようにするとき）、プラットフォーム918が秘密鍵を濫用しないことを信用する。

## 【0065】

コンテンツを濫用から完璧に守る権利管理システムはない。どんな権利管理システムも、十分な時間、スキル、リソース、および動機を有する敵によって破られる可能性がある。しかし、権利管理システムの性質上、コンテンツ所有者912は、処理チェーンに関係する様々なエンティティ（例えばこの例ではライセンス供与側914、識別証明書交付者916、およびプラットフォーム918）が、これらのエンティティに信用をおけるほど十分にうまく完全にそれぞれの鍵を保護するかどうかを決定することができる。したがってコンテンツのセキュリティは、どのエンティティを信用し、どのエンティティを信用しないかに直接に依存することが容易に理解できる。

10

20

30

40

50

## 【0066】

後述するように、本発明は、特定の信用関係のタイプを確立（または拒否）することに基づいてコンテンツを交付するためのシステムおよび方法を提供する。

## 【0067】

複数の識別サーバ間における信用の考慮

先に論じたように、誰を信用し誰を信用しないかを決定することによって部分的に、セキュリティスキームを定義することができる。これらの信用決定の一面は、識別証明書の特  
定の交付者によって交付されるこのような証明書を信用するかどうかを、ライセンス供与  
側が決定することである。この信用決定は重要である。というのも、ライセンス供与側は  
識別証明書の公開鍵（P U - E N T I T Y）でコンテンツを暗号化することになり、した  
がって、対応する秘密鍵（P R - E N T I T Y）が不正な人の手に落ちないようにする手  
段が講じられない限り、全世界が暗号化済みコンテンツにアクセスできるようになるから  
である。

10

## 【0068】

図10に、識別証明書1および2（参照番号1004（1）および1004（2））を交  
付する複数の識別サーバ1002（1）および1002（2）を示す。この例では、識別  
証明書1はエンティティ「ジョー」に向けたものであり、識別証明書2はエンティティ「  
フレッド」に向けたものである。このような識別は「ヘルソナ」と呼ぶこともできる。図  
示の例示的なヘルソナは個人だが、前の考察から、識別証明書は「グループエンティティ  
」または「グループヘルソナ」（「自動車部品部門」など）を定義することもできること  
は理解されるであろう。各識別証明書は、（相対的に）固有である鍵の対に関連し、識別  
証明書自体がこの鍵の対の公開部分を含む。したがって、識別証明書1は公開鍵P U - J  
O Eを含み、識別証明書2は公開鍵P U - F R E Dを含む。（図7に関連して先に論じた  
ように、識別証明書は鍵の対の秘密部分を含むこともできる。ただしユーザは秘密鍵への  
自由なアクセスを有するべきではないので、平文で含まないことが好ましい。）さらに、  
各識別証明書は署名を含む。署名は、（少なくとも）この公開鍵に対して取り入れられる  
。各証明書は、その交付者の署名を含む。したがって、識別証明書1は識別サーバ1の秘  
密鍵（P R - I S 1）で署名されており、識別証明書2は識別サーバ2の秘密鍵（P R -  
I S 2）で署名されている。識別サーバ1および2がこれらの識別証明書に署名すると  
き、これらは本質的に、これらの識別証明書についての秘密鍵が損なわれないよう保護する  
ことを表明している。

20

30

## 【0069】

識別サーバによっては、生み出したエンティティ用の秘密鍵のセキュリティを確保するこ  
とにおいてより優れている（またはより劣る）場合がある。図10の例では、識別サーバ  
1は「強いセキュリティプロシージャ」を有し、識別サーバ2は「弱いセキュリティプロ  
シージャ」を有する。これらのプロシージャの相対的な強度（または緩さ）は、どんな形  
を取る可能性もある。例えばおそらく、識別サーバ1は、物理的に安全なプラットフォーム  
鍵を有することがわかっているデバイスだけに秘密鍵をインストールし、識別サーバ2  
は、秘密鍵の取得側の信用を検証せずに、および／または秘密鍵がインストールされるこ  
とになるプラットフォームのタイプを検証せずに、平文で秘密鍵を渡す場合がある。これ  
らは、異なる識別サーバのセキュリティプロシージャの相対的な有効性がどれほど違うか  
ということの一例である。

40

## 【0070】

識別サーバ間のセキュリティにおけるこれらの違いにより、DRMサーバは、いくつかの  
識別サーバは信用でき、いくつかは信用できないと決定することができる。それによりD  
RMサーバは、信用する識別サーバによって署名された識別証明書だけにライセンスを交  
付することができる。図10の例では、識別サーバ1は強いセキュリティプロシージャを  
有するが、識別サーバ2は弱いセキュリティプロシージャを有するので、DRMサーバ3  
20は、識別サーバ1は信用するが識別サーバ2は信用しない。このためDRMサーバ3  
20は、識別サーバ1の秘密鍵で署名された識別証明書だけに対するライセンスを交付す

50

る。

#### 【0071】

図10では、サーバ1とサーバ2がそれぞれ「強い」「弱い」セキュリティプロシージャを有するものとして示してあるが、識別サーバの選択的な信用は「弱い」対「強い」に基づく必要はないことに留意されたい。例えば、サーバ1とサーバ2は、一方のサーバのセキュリティ機能が他方よりも明確に「強い」とは言えないとしても、単にセキュリティや認証などに関して異なる機能を有するだけでもよい。それでもやはりDRMサーバ320は、どの識別サーバを信用しどの識別サーバを信用しないかに関して選択をする資格を有する。例えば、2つのシステムが、両方とも強いセキュリティプロシージャを有するが、異なるようにユーザを認証する場合がある。例えば一方のシステムはスマートカードを必要とし、他方のシステムはX509証明書を必要とする。この違いは、DRMサーバ320を運営するエンティティにとって重要であることがある。したがって、識別サーバを信用するためにそのセキュリティの強度に基づいて選択することが本発明の典型的な使用方法であることは理解されたいが、これは、DRMサーバ320が信用するためにいくつかの識別サーバを選択して他の識別サーバを選択しないことの多くの理由の1つに過ぎない。

#### 【0072】

図11に、どの識別サーバを信用できるかについての決定が、2つの組織によって文書を共有できる方法に影響を及ぼす例を示す。2つの会社「会社A」および「会社B」は、その従業員が文書を共有できるようにしたいと思っており、これらの文書へのアクセスは、DRMシステムによって制御される。会社Aの従業員は、会社Aの識別サーバ1102によって交付される識別を有し、会社Bの従業員は、会社Bの識別サーバ1104によって交付される識別を有する。さらに、各会社は、DRM制御される文書を閲覧するためのライセンスを交付するそれ自体のDRMサーバを有する。通常、会社AのDRMサーバ1106は、会社Aの識別サーバ1102を信用するようにセットアップされ、会社BのDRMサーバ1104は、会社Bの識別サーバ1108を信用するようにセットアップされる。

#### 【0073】

典型的なシナリオでは、会社Aの従業員が、1つのコンテンツに対するライセンスを得るために、会社AのDRMサーバ1106に署名済み権利ラベルを提示する。この従業員は、会社Aの識別サーバ1102によって交付された識別（すなわち、鍵の対P U - E N T I T Y / P R - E N I T I T Yを含む識別証明書）を有する。署名済み権利ラベルによってこの従業員へのライセンス交付が許可されると仮定すると、会社AのDRMサーバ1106は、会社Aの識別サーバ1102を信用するので、この従業員の識別証明書のためのライセンスを作成することができる。しかし、会社Aのある従業員がコンテンツを発行し、この文書の使用許可を会社Bの従業員に与えたいとする。会社Aの従業員がこのコンテンツについての権利ラベルを生み出すとき、この権利ラベルは、コンテンツの許可ライセンス取得側の1人として会社Bの従業員のヘルソナを指定することができる。しかし、会社Bの従業員は会社Bの識別サーバ1104によって交付された識別証明書を有し、会社AのDRMサーバ1106は会社Bの識別サーバ1104を（まだ）信用しないので、会社Bのこの従業員がライセンスを得るために会社AのDRMサーバ1106に接触しても、会社AのDRMサーバ1106は、この従業員の識別証明書に対してライセンスを交付することができない。（図13～14に関連して後で論じるように、会社BのDRMサーバが会社Aで発行されたコンテンツに対するライセンスを交付できるようにすることも可能だが、そうするには会社Aと会社Bがそれらの秘密鍵を共有する必要があり、これは状況によっては望ましくない。）

#### 【0074】

解決法は、会社AのDRMサーバ1106と会社Bの識別サーバ1104との間に信用関係を確立することである。会社Aは、会社Bの識別サーバ1104が識別交付時に適切なセキュリティ手段をとると確信するステップを実施することが好ましい。会社Bの識別サーバが会社Aのセキュリティ基準を満たすことを会社Aが確信すると仮定すると、会社A

のDRMサーバ1106は、会社Bの識別サーバ1104を信用することができる。この信用関係により、会社Aの従業員は、会社Bの従業員にライセンス供与できる文書を発行することができる。同様に、会社BのDRMサーバ1108は、会社Aの識別サーバ1102を信用することができる。それにより会社Bの従業員は、会社Aにライセンス供与できる文書を発行することができる。

#### 【0075】

信用関係は、各DRMサーバが、信用される識別サーバのリスト1110および1112を維持するようにすることによって確立することができる。各識別サーバは、鍵の対を有し、その鍵の対の公開部分によって識別することができる。会社Aの識別サーバは鍵の対PU-A/PR-Aを有し、会社Bの識別サーバは鍵の対PU-B/PR-Bを有する。各識別証明書は、その証明書を交付した識別サーバの公開鍵証明書を含むことが好ましい。これにより所与の識別証明書について、DRMサーバは、その識別証明書中に表示される識別サーバ公開鍵を、信用される識別サーバのリスト上にある公開鍵と比較することにより、その識別証明書を交付した識別サーバを信用するかどうかを決定することができる。(識別サーバは、交付した識別証明書に含める別個の識別子を有することもある。DRMサーバは、公開鍵、識別子、またはその両方に基づいて、どの識別サーバが識別証明書を交付したかを決定することができる。)信用される識別サーバのリストは、「信用ヘルソナ領域」と呼ぶことができる。

#### 【0076】

したがって、会社Aは、会社Bの識別サーバを会社Aの信用リストに載せることにより、その従業員が会社Bの従業員に向けてコンテンツを発行できるようにすることができる(会社Bの従業員が会社Bの識別サーバによって交付された識別証明書を有すると仮定した場合)。同様に、会社Bは、会社Aの識別サーバをその信用リストに加えることができる。したがって図11には、公開鍵PU-Bが会社Aの信用リスト1110に加えられ、公開鍵PU-Aが会社Bの信用リスト1112に加えられていることが示してある。

#### 【0077】

通常なら信用される識別サーバによって交付された特定の証明書の除外先に論じたように、DRMサーバは、いくつかの識別サーバを選択的に信用したり/信用しなかったりする。この選択的な信用/不信モデルの注目すべき改良は、特定の識別サーバに与えられる一般的な信用から特定の識別を除外することに関するものである。例えばDRMサーバは、特定の識別サーバを一般に信用するが、特定のeメールアドレスやドメインなどに登録されたある種の証明書にはライセンスを交付したくない場合がある。唯一の例ではないがこの一例には、eメールアドレスに基づいて公衆に識別を交付する識別サーバの場合がある。MICROSOFT . NET PASSPORTは、このような識別サーバの例である。

#### 【0078】

図12に、識別サーバ1202および1204を示す。識別サーバ1202は、例えば、ユーザから提供されたeメールアドレスおよびパスワードに基づいて識別証明書を交付する、eメールアドレスに基づく公用の識別サーバとすることができる。例えば、ユーザは、eメールアドレス(例えばXXX@hottmail.com)およびパスワードを事前登録している。識別サーバ1202は、単にeメールアドレスおよびパスワードを入力するようユーザに促すだけでよく、ユーザが正しいeメールアドレス/パスワードの組合せを入力した場合は、それ以上の厳格なユーザ認証を要求することなく識別証明書を交付することができる。eメールアドレスに基づく公用の識別サーバ1202はまた、プラットフォームのセキュリティ機能を考慮せずに、ユーザの要求するどんなプラットフォームにも識別証明書をインストールすることができる場合があるという、セキュリティ上の欠点を有することがある。この技法は、識別証明書を交付する方法として相対的に安全でない方法であると考えられる。

#### 【0079】

対照的に、識別サーバ1204は高セキュリティ識別サーバである。識別サーバ1204

10

20

30

40

50



は、識別証明書を交付する前に、相対的に厳格なチェックを必要とする。例えば、ユーザは自分（および自分のコンピュータ）を（人間の）システム管理者に個人的に提示しなければならず、システム管理者は、そのコンピュータが十分に安全でありユーザがこのような識別を与えられる資格を有すると確信した場合に、サーバ1204によって識別証明書がユーザのコンピュータにインストールされるようにする。ユーザは、指紋やスマートカードなどを使用して自分を証明しなければならないこともある。あるいは、サーバ1204が会社のための識別サーバである場合、ユーザは、インターネットではなく社内イントラネットを介してサーバ1204にアクセスしなければならない。したがって、高セキュリティサーバ1204は、eメールアドレスに基づくサーバ1202よりも相対的により安全であることがわかる。

#### 【0080】

図12の例では、プラットフォーム1（参照番号1206）は、eメールに基づく識別サーバから識別証明書を入手し、プラットフォーム2（参照番号1208）は、高セキュリティの識別サーバから識別証明書を入手する。先に論じたように、各識別証明書はその交付者の公開鍵証明書を組み込んでおり、交付者の秘密鍵で署名されているので、これらの証明書の交付者は、証明書自体から決定することができる。（図12の例では、eメールアドレスに基づく公用サーバ1202は鍵の対P U - I S 1 / P R - I S 1を有し、高セキュリティの識別サーバ1204は鍵の対P U - I S 2 / P R - I S 2を有する。）したがって、プラットフォーム1および2がライセンス要求1210（それぞれの識別証明書を含む）をDRMサーバ320に送ることによって何らかのコンテンツに対するライセンスを得ようとするとき、DRMサーバは、どの識別サーバが識別証明書を交付したかを決定することができる。それにより、識別証明書を交付した識別サーバを信用するかどうかを決定することができる。先に論じたように、DRMサーバ320は、その信用する識別サーバのリストを調べることによってこの決定を行う。図12には、2つの代替例リスト1212および1214が示してある。（DRMサーバ320が2つの信用リストを同時に使用することが必要なのではなく、これらのリストは、DRMサーバ320が使用できるリストの代替例として共に図12に示すものである。）

#### 【0081】

リスト1212が使用される第1の例では、DRMサーバ320は、高セキュリティの識別サーバ1204を信用するが（このサーバの公開鍵証明書（P U - I S 2）が信用リスト1212上にあるため）、eメールアドレスに基づくサーバ1202はどんな状況下でも信用しない。

#### 【0082】

リスト1214が使用される第2の例では、DRMサーバ320は、高セキュリティの識別サーバ1204を信用し、およびeメールアドレスに基づく識別サーバ1202もいくつかの除外付きで信用する。例示的なリスト1214では、eメールに基づく公用の識別サーバ1202の信用は、特定の識別（j o e @ u n t r a c e a b l e a d d r e s s . c o m）または特定のドメイン名（ドメイン名k i g h - s e c u r i t y . c o mを有するすべてのアドレス）に交付された証明書を除外する。例えば、j o e @ u n t r a c e a b l e a d d r e s s . c o mは、コンテンツ泥棒として知られている人物（例えばDRMサーバ320を運営する会社の元従業員で不満を持っている者）であり、そのためDRMサーバ320は彼を信用しない。ドメイン名全体を除外したいと思う場合の理由は、いくぶん反直感的である。高セキュリティのサーバ1204が、会社の識別サーバであり、X X X @ k i g h - s e c u r i t y . c o mの形の識別を従業員に交付すると仮定する。会社は、自社の従業員を信用するが、従業員が会社の識別サーバ1204から得た識別証明書を実際に使用する場合にだけ従業員を信用したいことがある（このサーバはより強い認証プロセスまたは会社ポリシー施行機能を有するので）。会社は、（より弱いセキュリティの）サーバ1202を介して自分を識別したい従業員がいれば、その従業員は会社の何らかのポリシーを回避しようとしていると推定することができる。k i g h - s e c u r i t y . c o mを除外リストに載せることにより、高セキュリティのサー

10

20

30

40

50



パ１２０４を介して識別を得ることのできる人々はそのようにできることが保証され、また他の人々はメールアドレスに基づくサーバ１２０２を使用して自分を証明することができる。

#### 【００８３】

図１２および前の考察では、ｅメールに基づく公用の識別サーバに関して除外リストを使用することについて説明したが、除外リストの概念は、任意の識別サーバに適用することができることを理解されたい。例えば、会社１のＤＲＭサーバは、会社２の識別サーバによって交付された識別を信用するが、会社１は、自社の従業員には自社のサーバを介して識別を得るようにさせたい。このため会社１のＤＲＭサーバは、会社２の識別サーバについての除外リストを維持することができ、それにより、会社２の識別サーバによって交付される証明書だが×××@compa1.comの形のｅメールアドレスを指定する証明書があれば、この証明書はこの信用から除外される（会社１の従業員がドメインcompa1.com中のｅメールアドレスを有すると仮定した場合）。

#### 【００８４】

別のサーバの権利ラベルに基づくライセンス交付

前述のように、ユーザは一般に、ライセンスの基づく権利ラベルに署名したＤＲＭサーバと同じＤＲＭサーバからライセンスを得る。この理由の１つには、ライセンスはコンテンツ鍵（ＣＫ）を含まなければならないが、コンテンツ鍵はＤＲＭサーバの公開鍵ＰＵ－ＤＲＭを暗号化されてライセンス中に記憶されるということがある。したがって、対応する秘密鍵ＰＲ－ＤＲＭを保有するＤＲＭサーバだけが、ライセンスを生み出すために鍵ＣＫを得ることができる。（一実施形態では、対称鍵ＤＥＳ１が使用され、それにより署名済み権利ラベルはＤＥＳ１（ＣＫ）およびＰＵ－ＤＲＭ（ＤＥＳ１）を含む。ただしこの効果は同じであり、ＣＫは、ＰＲ－ＤＲＭを保有する識別によってしか回復することができない。）しかし、あるＤＲＭサーバが、別のＤＲＭサーバによって発行された１つのコンテンツに対してライセンスを交付できることが望ましい場合がある。

#### 【００８５】

このようなコンテンツの「相互ライセンス供与」を可能にする１つの方法は、第１のサーバ（コンテンツを発行したサーバ）が、その秘密鍵を別のサーバ（コンテンツをライセンス供与するサーバ）に提供するものである。秘密鍵を共有する際には注意を払わなければならない。ＤＲＭサーバの信用はその秘密鍵で表され、秘密鍵を有するものは誰でも、そのＤＲＭサーバに「扮する」（すなわち権利ラベルに署名しライセンスを交付する）ことができる。このため、第１のＤＲＭサーバの秘密鍵は、第２のＤＲＭサーバが秘密鍵を損ねることがないと確定できる場合にだけ、第２のＤＲＭサーバと共有すべきである。さらに、秘密鍵の移送は、移送中にうっかり誰かに漏れることがないように何らかの安全なスキームで行うことが好ましい。

#### 【００８６】

図１３に、２つのＤＲＭサーバの例と、どのようにして一方のＤＲＭサーバを使用して他方のＤＲＭサーバによって交付された権利ラベルに基づくライセンスを交付することができるかを示す。ＤＲＭサーバ１（参照番号１３２０）は、鍵の対ＰＵ－ＤＲＭ１／ＰＲ－ＤＲＭ１を有し、ＤＲＭサーバ２（参照番号１３２２）は、鍵の対ＰＵ－ＤＲＭ２／ＰＲ－ＤＲＭ２を有する。ユーザ１３０２は、暗号化済みコンテンツ１３０４と、このコンテンツについての署名済み権利ラベル１３０６とを有する。ユーザ１３０２は、このコンテンツに対するライセンスを得たいと思っている。署名済み権利ラベルは、暗号化された形のコンテンツ鍵ＣＫを含み、したがってＣＫは、ＰＲ－ＤＲＭ１を使用して対称鍵ＤＥＳ１を復号してからＤＥＳ１をＤＥＳ１（ＣＫ）に適用してＣＫを得ることによってのみ、得ることが可能である。言い換えれば、ＰＲ－ＤＲＭ１がなければ、コンテンツ１３０４に対するライセンスを交付するためにＣＫを得ることは不可能である。このため、ユーザ１３０２が署名済み権利ラベル１３０６をＤＲＭサーバ２に送っても、このＤＲＭサーバは、コンテンツ１３０６に対するライセンスを交付することはできない。

#### 【００８７】

10

20

30

40

50

しかし、DRMサーバ1がその秘密鍵PR-DRM1をDRMサーバ2と共有する場合（DRMサーバ1とDRMサーバ2を結ぶ点線で表す）、DRMサーバ2は、この秘密鍵を使用してCKを入手し、ライセンスを交付することができる。

【0088】

図13には、PR-DRM1をDRMサーバ1からDRMサーバ2に移送する例示的な方法の1つが示してある。図13の例では、PR-DRM1がDRMサーバ2の公開鍵で暗号化されて、PU-DRM2（PR-DRM1）が生み出されている。これによりPR-DRM1は、公衆の目から保護され、PU-DRM2（PR-DRM1）をDRMサーバ2の秘密鍵PR-DRM2で復号することによって回復することができる。秘密鍵を移送する安全な方法は他にもあり、図13に示す方法は例に過ぎないことを理解されたい。別の例としては、秘密鍵をディスクに収めて、信用される配達機関によって移送することができる。DRMサーバがアクセスできる秘密鍵のセットは、サーバの「信用文書領域」を定義する。

【0089】

図14に、このタイプの「相互ライセンス供与」スキームが有用な例を示す。会社1400は、地理的に異なる場所に散在している。部門A1402はアリゾナ州ウィンスローにあり、部門B1404はニュージャージー州アズベリーパークにある。実務上の理由で、各部門はそれぞれ、それ自体のDRMサーバ1406および1408を維持している。例えば、これらの部門は、DRMサーバを使用して1日あたり何千もの文書を発行および／またはライセンス供与しており、これらの発行／ライセンス供与の業務すべてを実施するために国を横断してデータを移送することに依存するのは実行可能なことではない。しかし、部門AとBは同じ会社1400内にあるので、部門Aの従業員は、部門Bの従業員にライセンス供与できるコンテンツを発行することができ、その逆も可能である。したがって、部門AとBにいるユーザ1410と1412はそれぞれ、DRMサーバAによって発行された何らかのコンテンツと、DRMサーバBによって発行された何らかのコンテンツを有する。例えば、ユーザ1412は、DRMサーバB上で発行された何らかのコンテンツをユーザ1410に送り、ユーザ1410は、DRMサーバA上で発行された何らかのコンテンツをユーザ1412に送ることができる。

【0090】

コンテンツの発行にどのサーバが使用されたかにかかわらず、各ユーザは、自分の部門にあるサーバに接触してライセンスを得る。したがって、ユーザ1410は、部門AのDRMサーバ1406にライセンスを要求し、ユーザ1412は、部門Bのサーバ1408にライセンスを要求する。各サーバは、そのサーバが発行したどんなコンテンツに対してもライセンスを交付することができる。というのは、そのようなコンテンツについての権利ラベルは、そのサーバの公開鍵で生成されたものだからである。さらに、両サーバがそれぞれの秘密鍵PR-DRMAおよびPR-DRMBを共有している限り、各サーバは、他方のサーバによって発行されたコンテンツに対するライセンスも交付することができる。

【0091】

ライセンス要求に対する信用を妥当性検査するプロセス

図15に、入来したライセンス要求に対する信用を妥当性検査するためにDRMサーバが実施する例示的なプロセスを示す。このプロセスは以下の概念を含む。（1）識別証明書は、信用される識別サーバによって交付されなければならない。（2）eメールアドレスに基づく公用の識別サーバによって識別証明書が交付される場合、証明書中で指定されるペルソナ（例えばjoe@university.edu.dress.com）またはドメイン（例えばsmith-secure.com）は、除外リスト上にあってはならない。（3）権利ラベルは、ライセンス供与するDRMサーバが関係を有するサーバによって交付されたものでなければならない。

【0092】

DRMサーバは、入来したライセンス要求（署名済み権利ラベルおよび識別証明書を含むことが好ましい）を受け取った後、この識別証明書が「信用ペルソナ領域」にあるかどうか

10

20

30

40

50

が、すなわち信用される識別サーバによって交付されたものかどうかを決定する（ステップ1502）。識別証明書が信用ベルソナ領域にない場合は、このライセンス要求は信用エラーにより拒否される（ステップ1512）。識別証明書が信用ベルソナ領域にある場合は、ステップ1504に進む。

#### 【0093】

ステップ1504で、DRMサーバは、この識別証明書を交付した信用される識別サーバに対して適用可能な除外リストがあるかどうかを決定する。前述の一例では、識別証明書の交付者は、MICROSOFT.NET PASSPORTサーバなどのeメールアドレスに基づく公用の識別サーバであり、DRMサーバは、そのサーバによって交付された識別証明書が特定のeメールアドレスおよび/またはドメインに交付されたものであれば、これらの識別証明書を異なるように扱うことを選択していた。ただし、除外リストは、信用ベルソナ領域中の任意の識別サーバに対して設定することができることを理解されたい。したがって、ステップ1504は一般に、特定の信用される識別サーバに関連する除外リストがあるかどうかを決定することを含む。

#### 【0094】

識別証明書を交付した識別サーバに関連する除外リストがない場合は、ステップ1508に進む。しかし、このような除外リストがある場合は、DRMサーバは、この証明書が交付されたベルソナに基づいて（例えばeメールアドレス、ドメイン、または識別証明書中で指定されるその他の識別子に基づいて）、この識別証明書を除外すべきかどうか（すなわちこのような証明書に対してライセンスを拒否しなければならないかどうか）を決定する（ステップ1506）。このような理由で識別証明書を除外しなければならない場合は、このライセンス要求は信用エラーにより拒否される（ステップ1512）。一方、識別証明書を除外しなければならないと除外リストが指定しない場合は、ステップ1508に進む。

#### 【0095】

ステップ1508で、DRMサーバは、ライセンス要求中で提供される署名済み権利ラベルが、ライセンス供与するDRMサーバの「信用文書領域」にあるDRMサーバによって交付されたものかどうかを決定する。先に論じたように、この「信用文書領域」は、（a）ライセンス供与要求を処理しているDRMサーバと、（b）要求を処理しているDRMサーバに秘密鍵を提供した（およびライセンス供与するDRMサーバが信用し続ける）他のDRMサーバとを含む。署名済み権利ラベルを交付したDRMサーバが信用文書領域にない場合は、このライセンス供与要求は信用エラーにより拒否される（ステップ1512）。一方、署名済み権利ラベルが信用文書領域中のサーバによって交付されたものである場合は、信用要求の妥当性が認められ、ライセンス要求は処理される（ステップ1510）。

#### 【0096】

最終的なライセンス交付は、図5A～5Bで先に説明したプロセスに従って行うことができる。さらに、図15に説明したプロセスは、図5A～5Bに説明したプロセスに追加するものとしてもよく、この2つのプロセスを共に織り交せてもよい。具体的には、ステップ1502、1504および1506は本質的に、要求側の識別を認証および許可する方法であり（図5Aのステップ604および606に示すように）、ステップ1508は本質的に、署名済み権利ラベルを妥当性検査するための特定の方法である（図5Bのステップ630に示すように）。

#### 【0097】

##### 結び

本発明に関連して実施されるプロセスを実現するのに必要なプログラミングは、比較的単純であり、関係するプログラミング界には明らかである。したがって、このようなプログラミングは本明細書に添付しない。この場合、任意の具体的なプログラミングを採用して、本発明の趣旨および範囲を逸脱することなく本発明を実施することができる。

#### 【0098】

10

20

30

40

50

さらに、本発明の好適実施形態に多くの変更および修正を加えることができ、このような変更および修正は本発明の趣旨を逸脱することなく加えることができることは、当業者なら理解するであろう。したがって、特許請求の範囲は、本発明の真の趣旨および範囲に含まれるこのような等価な変形をすべてカバーするものとする。

#### 【図面の簡単な説明】

【図 1】本発明を実施することのできる例示的および非限定的なコンピューティング環境を表すブロック図である。

【図 2】ディジタルコンテンツを発行するための、本発明によるシステムおよび方法の好適な実施形態の機能ブロック図である。

【図 3】図 3 の方法によって生成された署名済み権利ラベルの構造を示すブロック図である。 10

【図 4】権利管理されるディジタルコンテンツをライセンス供与するための、本発明によるシステムおよび方法の好適な実施形態の機能ブロック図である。

【図 5 A】権利管理されるディジタルコンテンツをライセンス供与するための、本発明による方法の好適な実施形態のフローチャートである。

【図 5 B】権利管理されるディジタルコンテンツをライセンス供与するための、本発明による方法の好適な実施形態のフローチャートである。

【図 6】本発明の特徴による権利管理システムをサポートする暗号機能を有するプラットフォームのブロック図である。

【図 7】本発明の態様による例示的な識別証明書のブロック図である。 20

【図 8】本発明の態様による例示的なライセンスのブロック図である。

【図 9】鍵保護層の間の関係、および信用のチェーンを示すブロック図である。

【図 10】本発明の態様による、識別サーバの選択的な信用を示すブロック図である。

【図 11】2つの組織間で文書を共有することを可能にする信用ヘルソナ領域の例示的な使用法のブロック図である。

【図 12】本発明の態様による、eメールに基づく公用の識別サーバを含む例示的なアーキテクチャのブロック図である。

【図 13】本発明の態様による、第 1 の DRM サーバが別の DRM サーバに代わってコンテンツをライセンス供与できるようにするために秘密鍵を共有することを示すブロック図である。 30

【図 14】2つの会社部門の間で保護コンテンツを相互ライセンス供与することを可能にする信用文書領域の例示的な使用法のブロック図である。

【図 15】本発明の態様による、ライセンス要求に対する信用を妥当性検査する例示的なプロセスを示す流れ図である。

#### 【符号の説明】

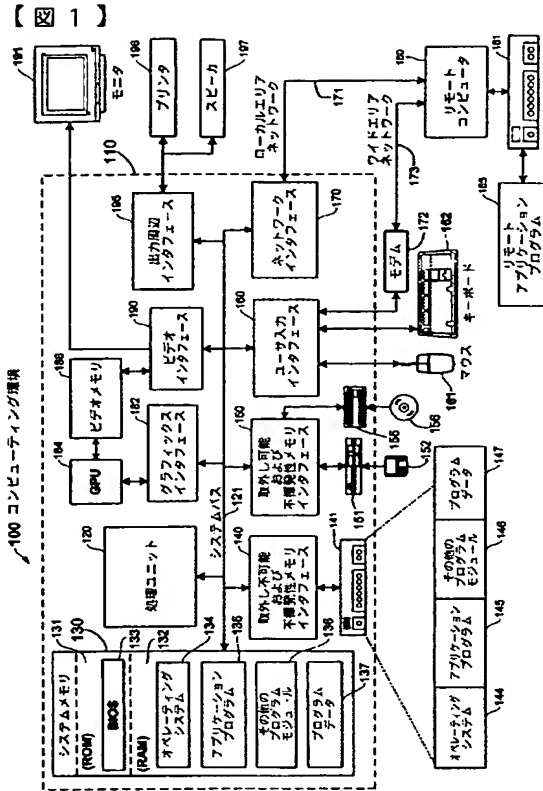
- 100 コンピューティング環境
- 110 コンピュータ
- 120 処理ユニット
- 121 システムバス
- 130 システムメモリ
- 131 ROM
- 132 RAM
- 133 BIOS
- 134 オペレーティングシステム
- 135 アプリケーションプログラム
- 136 その他のプログラムモジュール
- 137 プログラムデータ
- 140 取外し不可能および不揮発性メモリインタフェース
- 141 ハードディスクドライブ
- 144 オペレーティングシステム

1 4 5	アプリケーションプログラム	
1 4 6	その他のプログラムモジュール	
1 4 7	プログラムデータ	
1 5 0	取外し可能および不揮発性メモリインタフェース	
1 5 1	磁気ディスクドライブ	
1 5 2	磁気ディスク	
1 5 5	光ディスクドライブ	
1 5 6	光ディスク	
1 6 0	ユーザ入力インタフェース	
1 6 1	ポインティングデバイス	10
1 6 2	キーボード	
1 7 0	ネットワークインタフェース	
1 7 1	ローカルエリアネットワーク (LAN)	
1 7 2	モデム	
1 7 3	ワイドエリアネットワーク (WAN)	
1 8 0	リモートコンピュータ	
1 8 1	メモリ記憶デバイス	
1 8 2	グラフィックスインタフェース	
1 8 4	グラフィックス処理ユニット (GPU)	
1 8 5	リモートアプリケーションプログラム	20
1 8 6	ビデオメモリ	
1 9 0	ビデオインタフェース	
1 9 1	モニタ	
1 9 5	出力周辺インタフェース	
1 9 6	プリンタ	
1 9 7	スピーカ	
3 0 0	クライアント	
3 0 2	コンテンツ作成アプリケーション	
3 0 2	クライアントアプリケーション	
3 0 4	暗号化済みデジタルコンテンツ	30
3 0 6	DRMクライアントAPI	
3 0 8	署名済み権利ラベル (SRL)	
3 1 0	権利管理されるデジタルコンテンツ	
3 1 2	復号されたデジタルコンテンツ	
3 2 0	DRMサーバ	
3 3 0	通信ネットワーク	
6 0 2	プラットフォーム	
6 0 4	暗号モジュール	
7 0 2	識別証明書	
8 0 2	ライセンス	40
9 0 2	コンテンツ	
9 0 4	コンテンツ鍵	
9 0 6	エンティティ鍵の対	
9 0 8	プラットフォーム鍵の対	
9 1 2	コンテンツ所有者	
9 1 4	ライセンス供与側	
9 1 6	エンティティ証明書交付者	
9 1 8	プラットフォーム	
1 0 0 2 (1)	識別サーバ 1	
1 0 0 2 (2)	識別サーバ 2	50

1 0 0 4 ( 1 ) 識別証明書 1  
1 0 0 4 ( 2 ) 識別証明書 2  
1 1 0 2 会社 A の識別サーバ  
1 1 0 4 会社 B の識別サーバ  
1 1 0 6 会社 A の DRM サーバ  
1 1 0 8 会社 B の DRM サーバ  
1 1 1 0 信用される識別サーバのリスト  
1 1 1 2 信用される識別サーバのリスト  
1 2 0 2 識別サーバ  
1 2 0 4 高セキュリティの識別サーバ  
1 2 0 6 フラットフォーム 1  
1 2 0 8 フラットフォーム 2  
1 2 1 0 ライセンス要求  
1 2 1 2 信用される識別サーバのリスト  
1 2 1 4 信用される識別サーバのリスト  
1 3 2 0 DRM サーバ 1  
1 3 2 2 DRM サーバ 2  
1 3 0 2 ユーザ  
1 3 0 4 暗号化済みコンテンツ  
1 3 0 6 署名済み権利ラベル  
1 4 0 2 部門 A  
1 4 0 4 部門 B  
1 4 0 6 DRM サーバ A  
1 4 0 8 DRM サーバ B  
1 4 1 0 部門 A のユーザ  
1 4 1 2 部門 B のユーザ

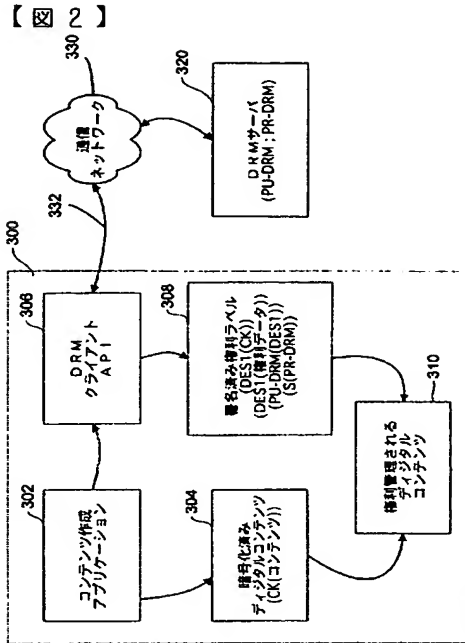
10

20

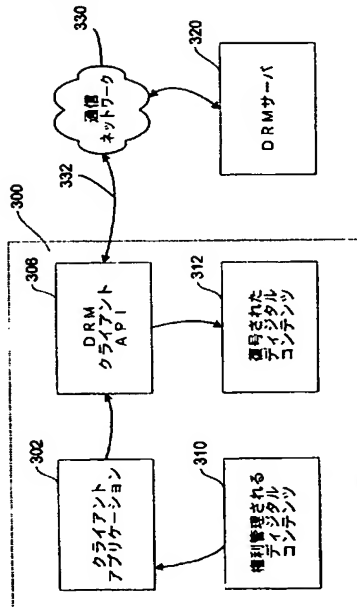


【図 3】

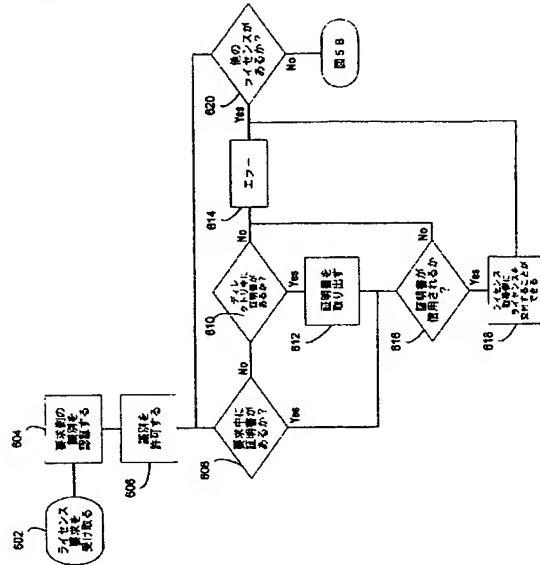
SRL 308
コンテンツ情報
DRMサーバ情報
-(PU-DRM(DES1))
- 参照情報
-- URL
-- フォールバック
権利ラベル情報
(DES1(権利データ))
(DES1(CK))
S (PR-DRM)



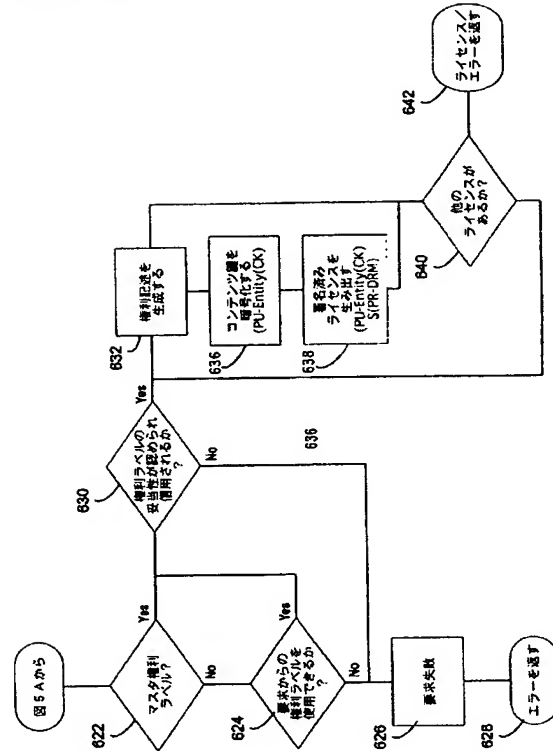
【図 4】



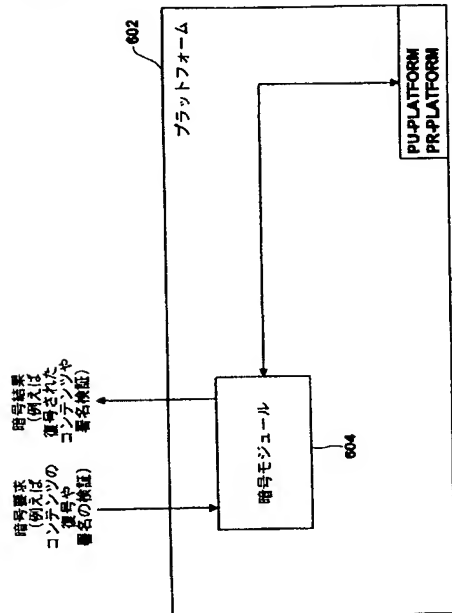
【図 5 A】



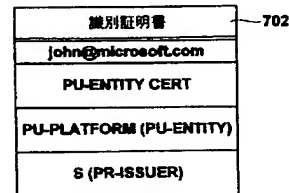
【図 5 B】



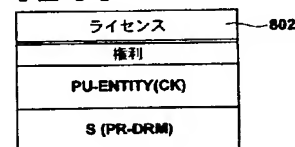
【図 6】



【図 7】

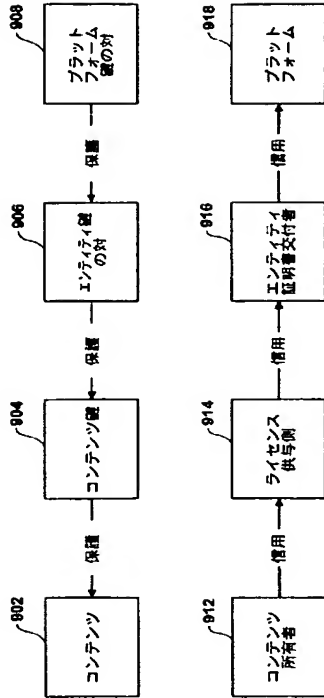


【図 8】

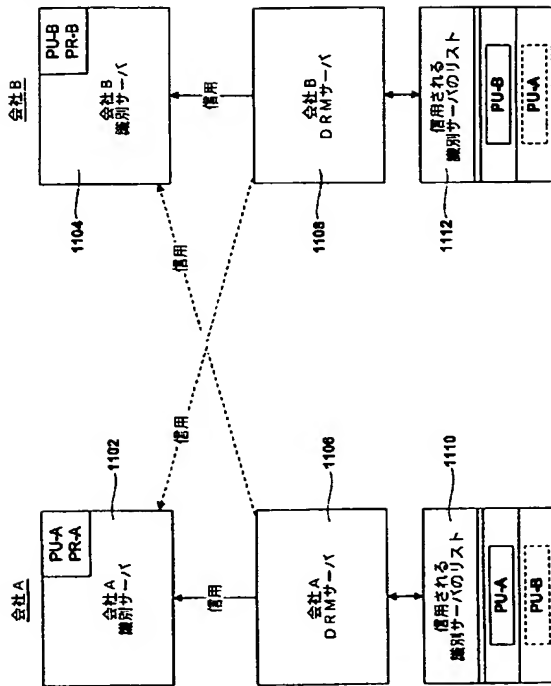




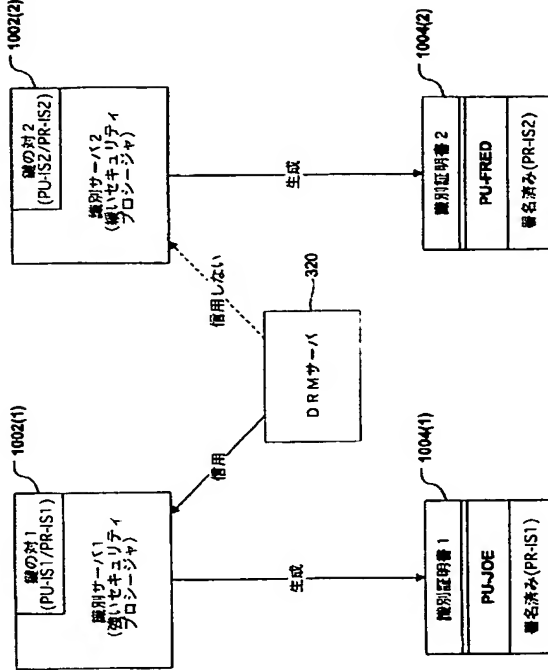
【図 9】



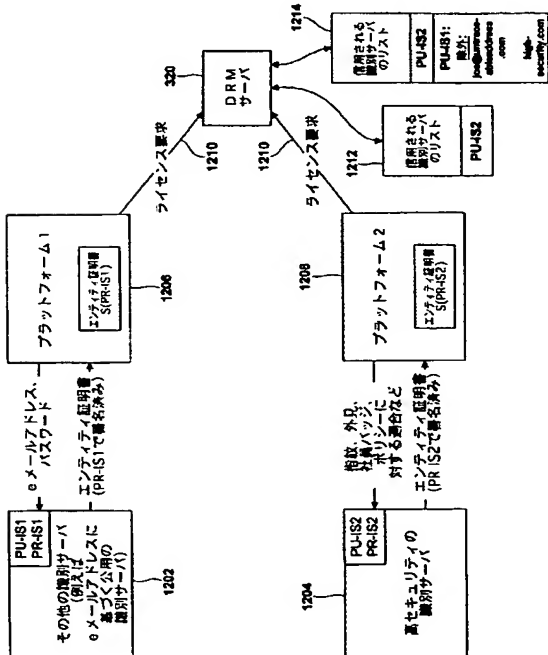
【図 11】



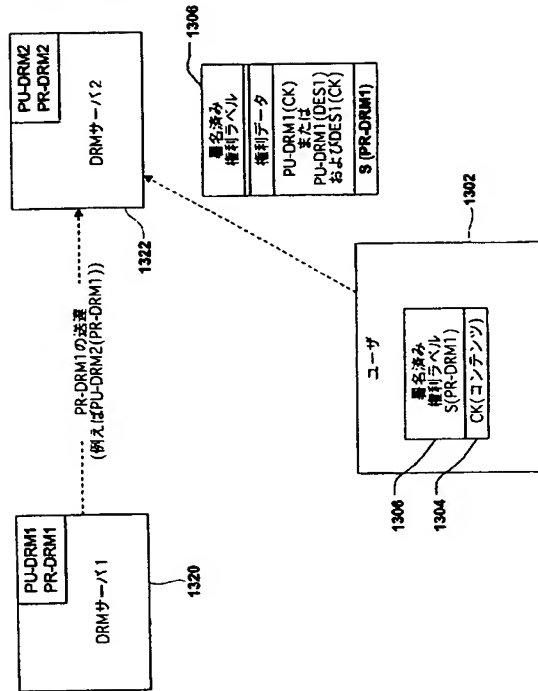
【図 10】



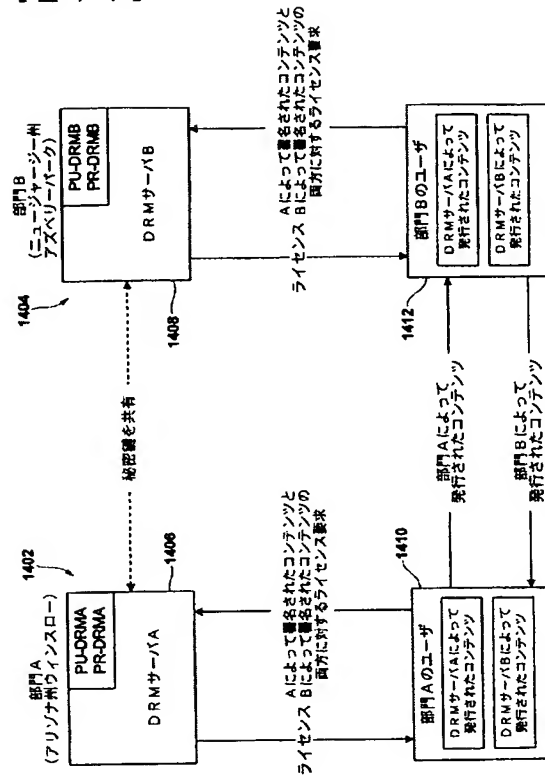
【図 12】



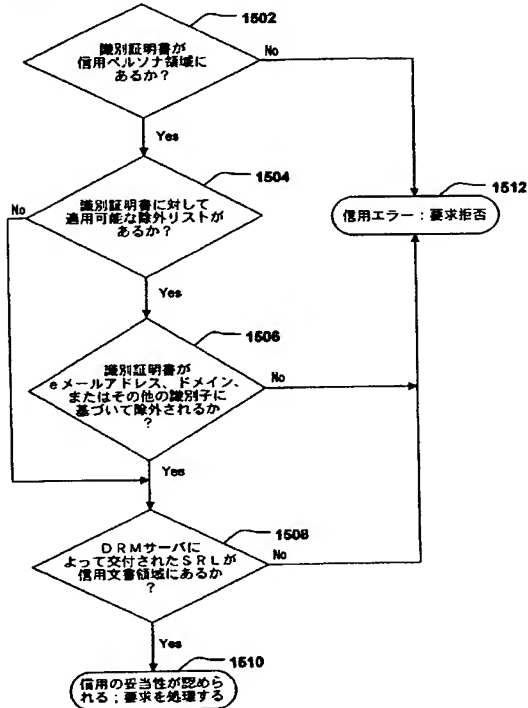
【図 13】



【図 14】



【図 15】



## フロントページの続き

(51)Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
	G 0 6 F 17/60	Z E C
	H 0 4 L 9/00	6 0 1 F
	H 0 4 L 9/00	6 0 1 B

(72)発明者 ビーター デビッド ワックスマン  
 アメリカ合衆国 9 8 0 0 4 ワシントン州 ヘルビュー ノースイースト 2 8 フレイス 1  
 0 0 0 8

(72)発明者 トーマス ケー. リンデマン  
 アメリカ合衆国 9 8 0 5 2 ワシントン州 レッドモンド ノースイースト 1 8 8 フレイス  
 1 7 2 2 5

(72)発明者 フランク バイラム  
 アメリカ合衆国 9 8 1 0 1 ワシントン州 シアトル ウエスタン アベニュー 1 2 0 0 ナ  
 ンバー 1 2 1 0

Fターム(参考) 5B017 AA07 BA06 BA07 CA16  
 5B085 AE09 AE23 AE29 BG01 BG04 BG07  
 5J104 EA05 EA17 EA19 PA10

**THIS PAGE BLANK (USPTO)**